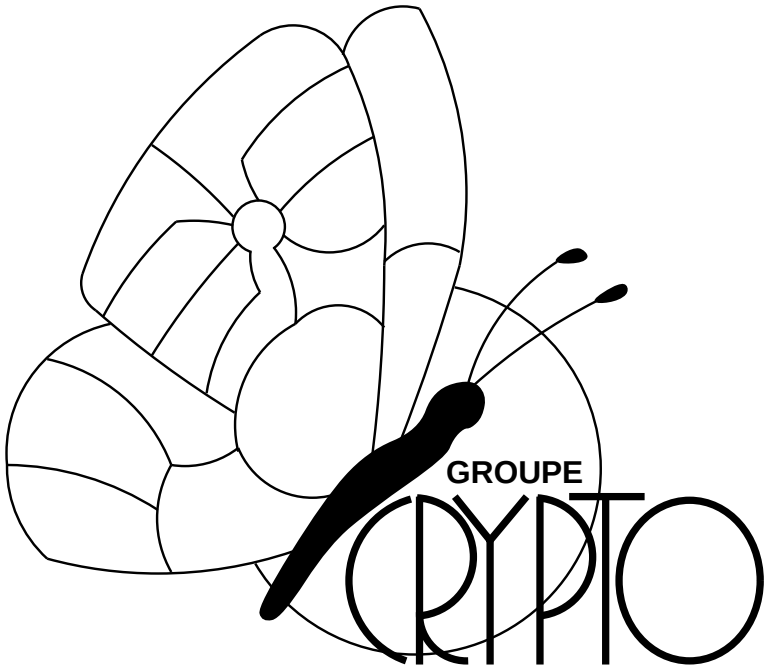
UCL
Université
catholique
de Louvain

REGARDS

UCL Crypto Group Technical Report Series

Introduction élémentaire à la théorie des courbes elliptiques

Marc Joye



http://www.dice.ucl.ac.be/crypto/

Technical Report
CG–1995/1

Place du Levant, 3
B-1348 Louvain-la-Neuve, Belgium

Phone: (+32) 10 472541
Fax: (+32) 10 472598

Introduction élémentaire à la théorie des courbes elliptiques

Marc Joye

25 juin 1995

Département de Mathématique (AGEL), Université catholique de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
E-mail: joye@agel.ucl.ac.be

La théorie des courbes elliptiques a connu un récent regain d'intérêt grâce à l'émergence de la cryptographie. Tout a commencé lorsque Lenstra a découvert un algorithme de factorisation polynomial sur ces structures. Ensuite, en 1985, Koblitz et Miller ont proposé indépendamment d'adapter les protocoles cryptographiques existant sur les courbes elliptiques.

Ce rapport est organisé comme suit. Les trois premières parties fournissent les bases nécessaires. Le lecteur ayant une certaine culture mathématique peut commencer la lecture à la partie IV. Celui-ci introduit la théorie des courbes elliptiques.

Nous verrons qu'à toute courbe elliptique est associée une structure de groupe. Par ailleurs, nous montrerons qu'une courbe elliptique est birationnellement équivalente à une forme particulière : les équations de Weierstrass.

Enfin, le dernière partie propose quelques applications liées aux courbes elliptiques. Nous verrons comment il est possible de tester la primalité d'un nombre et s'il n'est pas premier, comment le factoriser. Ces méthodes sont basées sur le théorème de Hasse qui donne une approximation de la cardinalité d'une courbe elliptique. Finalement, les schémas de Diffie-Helman et d'El Gamal seront adaptés pour pouvoir être utilisés sur les courbes elliptiques.

Bonne lecture.

CG–1995/1

Table des matières

Partie I
Notions élémentaires d'algèbre supérieure

Résumé. Dans cette partie seront revues les définitions d'un groupe, d'un anneau et d'un corps. Plusieurs théorèmes importants sur ces structures seront également abordés. Enfin, les définitions d'homomorphisme et d'isomorphisme seront rappelées. Afin de faciliter la compréhension, de nombreux exemples illustreront les définitions.

I.1 Groupes

Définition 1. Un *groupe* est un couple formé d'un ensemble G et d'une loi de composition $(x, y) \mapsto xy$ sur l'ensemble G. Ces données doivent vérifier les trois conditions :

- $\forall x, y, z \in G : (xy)z = x(yz)$ (associativité) ;
- $\exists 1 \in G$ tel que $\forall x \in G : x1 = 1x = x$ (existence d'un élément neutre) ;
- $\forall x \in G, \exists x^{-1} \in G$ tel que $x^{-1}x = xx^{-1} = 1$ (existence d'un élément inverse pour tout élément du groupe).

Si la loi de groupe est commutative, le groupe est appelé *groupe commutatif* (ou *abélien*).

Pour un groupe commutatif, nous utilisons l'écriture additive au lieu de l'écriture multiplicative, i.e. la loi de composition est $(x, y) \mapsto x + y$.
Dans cette notation, l'élément neutre est habituellement noté 0 et l'inverse d'un élément x est noté $-x$.

Exemple 1. L'ensemble des entiers muni de la loi de composition $(x, y) \mapsto x + y$, i.e. le groupe additif $\mathbb{Z}$ noté $(\mathbb{Z}, +)$, forme un groupe commutatif.

Exemple 2. L'ensemble des réels non nuls muni de la loi de composition $(x, y) \mapsto xy$, i.e. le groupe multiplicatif $\mathbb{R}^*$ noté $(\mathbb{R}^*, \cdot)$, forme un groupe commutatif.[†]

[†]Lorqu'un ensemble est muni d'une astérisque, cela signifie l'ensemble des éléments inversibles de l'ensemble.

Définition 2. Une partie H d'un groupe G est un *sous-groupe* de G si H est non vide et si $(x \in H, y \in H \Rightarrow xy^{-1} \in H)$.

Exemple 3. Le groupe additif $\mathbb{Z}$ est un sous-groupe du groupe additif $\mathbb{R}$.

Théorème 3. *Tout sous-groupe M du groupe addidif $\mathbb{Z}$ est de la forme $M = m\mathbb{Z}$ où m est le plus petit entier positif de M.*

Preuve. (i) Si $M = \{0\}$, alors il suffit de prendre $m = 0$.
(ii) Nous pouvons donc supposer $M \neq \{0\}$. Soit d le plus entier strictement positif de M. Par l'absurde, si un élément x de M n'est pas un multiple de d, alors $\exists k : kd < x < (k+1)d$. Mais alors $y = x - d - \cdots - d = x - kd \in M$. Or $0 < y = x - kd < d$, ce qui contredit le fait que d est le plus entier positif de M. □

Remarque. Un sous-groupe commutatif dont la loi de composition est noté additivement et dont l'élément neutre est noté 0 est appelé un *module*. Le théorème précédent peut alors se formuler : *Tout module d'entiers $M \neq \{0\}$ est généré par son plus petit entier strictement positif.*

Corollaire 4. *Soient a, b et c des nombres entiers. L'équation diophantienne*

$$ax + by = c$$

admet des solutions entières si et seulement si le plus grand diviseur commun de a et de b divise c.

Notation. Soient a et b deux entiers. Le plus grand commun diviseur de a et de b est noté $\text{pgcd}(a, b)$ ou encore (a, b). Si a divise b, alors nous écrivons $a|b$.

Preuve. Les entiers de la forme $ax+by$ appartiennent à M dont le générateur est $d = (a, b)$. Pour que $ax+by = c$ ait des solutions entières, il faut et il suffit que c appartienne à M, c.-à-d. que c soit un multiple entier de (a, b). □

Corollaire 5 (Théorème de Bezout). *Les entiers a et b sont premiers entre eux si et seulement si $\exists u, v \in \mathbb{Z} : au + bv = 1$.*

Preuve. Trivial par le corollaire 4. □

Définition 6. Soit G un groupe comportant n éléments. Alors G est un *groupe fini* si n est fini ; et dans ce cas, n désigne l'*ordre* du groupe.

Un élément a de G est d'*ordre l* si l est le plus entier strictement positif tel que $a^l = 1$.

Théorème 7 (Théorème de Lagrange). *Soit G un groupe fini d'ordre n. Tout élément a de G satisfait à $a^n = 1$.*

Preuve. Notons l l'ordre de l'élément a.
(i) Construisons l'ensemble $C_0 = \{a, a^2, a^3, \ldots, a^l = 1\}$. Tous les éléments de C_0 sont forcément distincts ; sinon il existerait $0 < s < t < l$ tels que $a^{t-s} = 1$, ce qui contredit la minimalité de l. Si $G = C_0$, alors $n = l$ et le théorème est démontré.
(ii) Construisons le *coensemble* C_1 à partir d'un élément $b_1 \in G \backslash C_0$:

$$C_1 = \{ab_1, a^2b_1, a^3b_1, \ldots, a^lb_1 = b_1\}.$$

Tous les éléments de C_1 sont distincts entre eux par la minimalité de l et sont distincts de ceux de C_0 car $b_1 \notin C_0$. Si $G = C_0 \cup C_1$, alors $n = 2l$ et le théorème est démontré.
(iii) Nous recommençons de même jusqu'à ce que $G = C_0 \cup C_1 \cup \ldots \cup C_h$ où $C_i = \{ab_i, a^2b_i, a^3b_i, \ldots, a^lb_i = b_i\}$ avec $b_i \in G \backslash \cup_{k=0}^{i-1} C_k$. Nous obtenons donc $n = (h+1)\,l$ et le théorème est démontré. □

Le théorème de Lagrange montre que l'ordre d'un élément divise toujours l'ordre de son groupe. S'il existe un élément dont l'ordre est égal à celui de son groupe, alors le groupe est appelé *groupe cyclique* et un tel élément est appelé *générateur* du groupe.

I.2 Anneaux et corps

Définition 8. Un *anneau* est un triplet formé d'un ensemble K et de deux lois de composition $(x, y) \mapsto xy$ et $(x, y) \mapsto x + y$ sur l'ensemble K. Ces données doivent vérifier les trois conditions suivantes :

- $(K, +)$ est un groupe commutatif ;
- la loi de composition $(x, y) \mapsto xy$ est associative et admet un élément neutre 1 ;
- $\forall x, y, z \in K : x(y + z) = xy + yz$ (distributivité).

Si la loi de composition $(x, y) \mapsto xy$ est commutative, alors l'anneau est *commutatif*.

Exemple 4. L'ensemble des entiers muni des lois composition habituelles (addition et multiplication) forme un anneau commutatif : l'*anneau des entiers rationnels*.

Définition 9. Une partie A d'un anneau K est un *sous-anneau* de K si A est un sous-groupe du groupe additif K, si $(x, y \in A \Rightarrow xy \in A)$ et si $1 \in A$.

Définition 10. Un anneau K est un *domaine intégral* si pour $x, y, z \in K$:

$$(xy = xz \text{ et } x \neq 0 \Rightarrow y = z).$$

Définition 11. Soit un anneau K. Nous dirons que K est un *corps* si tout élément non nul de K est inversible.[†]

L'ensemble des éléments inversibles de K est noté K^*. Si nous munissons cet ensemble K^* de la loi de composition $(x, y) \mapsto xy$, il désigne le *groupe multiplicatif de l'anneau* K. Dans le cas où K est un corps, alors nous avons $K^* = K \backslash \{0\}$.

Exemple 5. Les anneaux $\mathbb{Q}$ et $\mathbb{R}$ sont des corps, appelés respectivement *corps des nombres rationnels* et *corps des nombres réels.*

Exemple 6. Par contre, l'anneau $\mathbb{Z}$ n'est pas un corps car les seuls éléments non nuls qui sont inversibles sont 1 et -1, i.e. $\mathbb{Z}^* = \{1, -1\}$.

Définition 12. Un anneau K est *intègre*, ou encore K est un *anneau d'intégrité*, si pour $x, y \in K$:

$$(xy = 0 \Rightarrow x = 0 \text{ ou } y = 0).$$

Tous les anneaux ne sont pas intègres. Si $xy = 0$ n'implique pas $x = 0$ ou $y = 0$, les éléments x et y sont appelés *diviseurs de zéro.*

Exemple 7. L'anneau $(\mathbb{Z}/4\mathbb{Z})$ n'est pas intègre car $2 \cdot 2 = 0$. Une équation de degré n peut par conséquent avoir plus de n racines dans $(\mathbb{Z}/4\mathbb{Z})$.

Proposition 13. *Si K est un corps, alors K est un domaine intégral et un anneau d'intégrité.*

Preuve. (i) Montrons que K est un domaine intégral.
Soient $x, y, z \in K$ avec $x \neq 0$, alors

$$xy = xz \Rightarrow x^{-1}xy = x^{-1}xz \Rightarrow y = z.$$

(ii) Montrons que K est un anneau d'intégrité.
Soient $x, y \in K$ avec $x \neq 0$, alors

$$xy = 0 \Rightarrow x^{-1}xy = 0 \Rightarrow y = 0.$$

□

[†]Dans la définition du corps, il faut en plus exiger que $1 \neq 0$; un corps possède donc au moins deux éléments.

Définition 14. Une partie I d'un anneau K est un *idéal à gauche* de K si

1. I est un sous-groupe du groupe additif K ;
2. $\forall a \in K, \forall x \in I : ax \in I$.

De même, un *idéal à droite* d'un anneau K est un sous-groupe du groupe additif K tel que $\forall a \in K, \forall x \in I : xa \in I$. Si K est commutatif, on parle alors d'*idéal bilatéral* ou tout simplement d'*idéal*.

Proposition 15. *Si K est un corps, alors les seuls idéaux à gauche de K sont $\{0\}$ et K.*

Preuve. (i) $I = \{0\}$ est un idéal à gauche de K, car $\forall a \in K : a0 = 0 \in I$.
(ii) Supposons que I contienne un élément non nul x. Alors x est inversible : $x^{-1}x = 1 \in I$. Par conséquent, $a1 = a$ pour tout $a \in K$, d'où $I = K$. □

Définition 16. Un *anneau principal* est un anneau d'intégrité commutatif dont tous les idéaux sont principaux.[†]

Remarque. En anglais, le mot *field* est également utilisé. Ce mot est parfois traduit par "champ" et désigne un corps commutatif.

I.3 Homomorphismes et isomorphismes

Définition 17. Soient deux groupes G et H. L'application $f : G \to H$ est un *homomorphisme* de G dans H si

$$\forall x, y \in G : f(xy) = f(x)f(y). \tag{I.1}$$

Si, dans la relation (I.1), nous prenons $y = 1$, alors $f(1) = 1$ et si nous prenons $y = x^{-1}$, alors $f(x^{-1}) = (f(x))^{-1}$.

Remarque. Dans la définition, nous avons utilisé l'écriture multiplicative pour les groupes G et H. Si les groupes sont notés additivement, il faut bien sûr adapter la définition en conséquence. Par exemple, si le groupe G est noté additivement et le groupe H multiplicativement, alors la relation (I.1) devient $f(x + y) = f(x)f(y)$.

[†]Dans un anneau commutatif K, un idéal principal est l'ensemble des multiples de $x\,(\in K)$ dans K, i.e. $I = xK$.

Exemple 8. Soient G le groupe additif $\mathbb{Z}$, H un groupe multiplicatif quelconque et a un élément de H. L'application $f : \mathbb{Z} \to H : n \mapsto a^n$ est un homomorphisme de $\mathbb{Z}$ dans H. En effet, $f(n_1 + n_2) = a^{n_1+n_2} = a^{n_1}a^{n_2} = f(n_1)f(n_2)$.

Définition 18. Soient deux groupes G et H. Tout homomorphisme bijectif de G dans H est appelé *isomorphisme* de G dans H. Nous disons alors que les groupes G et H sont *isomorphes*.

Exemple 9. La fonction "logarithme" est un isomorphisme du groupe multiplicatif $\mathbb{R}_+^*$ dans le groupe additif $\mathbb{R}$: $\log(xy) = \log(x) + \log(y)$.

Un isomorphisme d'un groupe G dans lui-même est un *automorphisme*.

Définition 19. Soient deux anneaux K et L. L'application $f : K \to L$ est un *homomorphisme* de K dans L si $\forall x, y \in K$

$$f(x + y) = f(x) + f(y) \text{ et } f(xy) = f(x)f(y).$$

Définition 20. Soient deux anneaux K et L. Tout homomorphisme bijectif de K dans L est appelé *isomorphisme* de K dans L. Nous disons alors que les anneaux K et L sont *isomorphes*.

À retenir.

- Un *groupe* est un ensemble muni d'une loi de composition appelée *multiplication* qui permet de multiplier deux éléments de l'ensemble. Si la loi de composition est *commutative*, alors elle est appelée *addition*.
- Un *anneau* est un ensemble muni de deux lois de composition appelées *multiplication* et *addition* telles que la multiplication est *distributive* par rapport à l'addition et qui permettent de multiplier et d'additionner des éléments de l'ensemble.
- Un anneau K est *domaine intégral* si pour $x, y, z \in K$: ($xy = xz$ et $x \neq 0 \Rightarrow y = z$).
- Un *corps* est un anneau dont tous les éléments non nuls sont *inversibles*.
- Une application f d'un groupe G dans un groupe H est un *homomorphisme de groupes* si $\forall x, y \in G : f(xy) = f(x)f(y)$.
- Une application f d'un anneau K dans un anneau L est *homomorphisme d'anneaux* si $\forall x, y \in K : f(xy) = f(x)f(y)$ et $f(x + y) = f(x) + f(y)$.
- Un *isomorphisme* est un homomorphisme bijectif.

Partie II
Corps finis

Résumé. Cette partie a pour but de montrer comment construire un corps à partir d'un domaine euclidien. Ensuite, il sera démontré que la cardinalité d'un corps fini est toujours une puissance d'un nombre premier. En particulier, ce théorème permettra de représenter les éléments de $\mathbb{F}_{p^m}$ comme des m-uples de $\mathbb{F}_p$.

II.1 Corps et domaine euclidien

Définition 21. Un *domaine euclidien* est un domaine intégral D muni de la fonction $g : D \to \mathbb{N}, a \mapsto g(a)$, telle que

- $g(a) \leq g(ab)$ si $b \neq 0$;
- $\forall a, b \neq 0 \in D, \exists q, r \in D : a = qb + r$ avec $r = 0$ ou $g(r) < g(b)$.

Exemple 10. L'ensemble des entiers $\mathbb{Z}$ avec $g(n) = |n|$ forme un domaine euclidien.

Exemple 11. L'anneau des polynômes à une variable à coefficients dans K, i.e. $D = K[x]$, avec $g(f(x)) = \text{degré}(f)$ forme un domaine euclidien.

Théorème 22. *Soit $B = \{b_1, b_2, \ldots, b_n\}$ un sous-ensemble fini d'un domaine euclidien D, alors B a un plus grand commun diviseur d qui peut être exprimé comme une combinaison linéaire des b_i :*

$$d = \sum_{i=1}^{n} \lambda_i b_i.$$

Preuve. (i) Construisons l'ensemble $S = \{\sum_{i=1}^{n} \mu_i b_i \mid \mu_i \in D\}$. Soit d un élément non nul de S pour lequel $g(d)$ est minimal. Comme $d \in S$, $d = \sum_{i=1}^{n} \lambda_i b_i$. Montrons que ce d ainsi défini est un diviseur commun de B ; cela revient à montrer que $d|b_i$ pour $i = 1, 2, \ldots, n$. Nous savons, par la définition 21, que $b_i = dq_i + r_i$ pour $i = 1, 2, \ldots, n$ avec $r_i = 0$ ou $g(r_i) < g(d)$. Or comme $g(d)$ est minimal, cela implique que $r_i = 0$, c.-à-d. $d|b_i$ pour $i = 1, 2, \ldots, n$.
(ii) Il reste à montrer que c'est le plus grand diviseur. Par l'absurde, supposons qu'il existe e un diviseur commun de B, i.e. $\exists q_i'$ tels que $b_i = eq_i'$ pour $i = 1, 2, \ldots, n$. Or d est une combinaison linéaire des b_i, donc $d = \sum_{i=1}^{n} \lambda_i b_i = e \sum_{i=1}^{n} \lambda_i q_i'$, ce qui signifie que d est un multiple de e. □

Le théorème précédent permet d'étendre le théorème de Bezout aux domaines euclidiens.

Corollaire 23 (Théorème de Bezout étendu). *Les éléments a et b d'un domaine euclidien D sont premiers entre eux si et seulement $\exists u, v \in D$: $au + bv = 1$.*

Preuve. Trivial. □

Théorème 24. *Soit D un domaine euclidien. Si $p \in D$ est premier, alors $K = D \bmod p$ est un corps.*

Preuve. Soit a un élément non nul de D. Comme p est premier, par le corollaire 23, $\exists u, v \in D : au + pv = 1$; et donc $au \equiv 1 \pmod{p}$. Tout élément non nul de $D \bmod p$ est par conséquent inversible. □

Nous sommes maintenant en mesure de construire des corps.

Exemple 12. Si nous prenons $D = \mathbb{Z}$ et un quelconque nombre premier p, nous obtenons un corps fini qui contient exactement p éléments $\{0, 1, \ldots, p-1\}$.

Notation. Le corps ainsi défini est habituellement noté $\mathbb{F}_p$ ou encore $GF(p)$.[†]

Exemple 13. Prenons $D = \mathbb{R}[x]$, l'ensemble des polynômes à une variable à coefficients réels et $p = x^2 + 1$, un polynôme irréductible dans $\mathbb{R}$. Les éléments de $D \bmod p$ sont des polynômes du premier degré. Soient $f(x) = ax + b$ et $f'(x) = a' + b'x$ deux éléments de $D \bmod p$. L'addition de $f(x)$ et de $f'(x)$ donne

$$f(x) + f'(x) = (a + a') + (b + b')x.$$

La multiplication, quant à elle, donne

$$f(x)f'(x) = aa' + (ab' + a'b)x + bb'x^2 = (aa' - bb') + (ab' + a'b)x.$$

Nous voyons que si nous remplaçons x par i, nous retrouvons les opérations définies sur les nombres complexes. Nous avons donc construit $\mathbb{C}$, le *corps des nombres complexes.*

[†] GF pour Galois Field.

II.2 Cardinalité d'un corps fini

Théorème 25. *Soit un corps fini F. Alors le nombre q d'éléments de F est une puissance d'un nombre premier p, i.e. $q = p^m$.*

Preuve. (i) Construisons la suite $\{u_i\}$ dans F comme suit :

$$\begin{cases} u_0 = 0 \\ u_n = u_{n-1} + 1, \text{ pour } n \geq 1 \end{cases}. \tag{II.1}$$

Comme F est fini, tous les éléments u_n ne sont pas distincts. Soit $u_k = u_{k+c}$, la première répétition rencontrée, c.-à-d. les éléments $u_0, u_1, \ldots, u_{k+c-1}$ sont tous distincts. Or, par (II.1), $u_{k+c} = u_k + u_c$, et donc $u_c = 0$. Il s'ensuit que le premier élément répété est 0 et que les éléments de la suite $\{u_0, u_1, \ldots, u_{c-1}\}$ sont tous distincts.
Montrons que c est premier. Remarquons d'abord que $c \geq 2$ par définition d'un corps. Par l'absurde, supposons que $c = ab$, avec $1 < a, b < c$. La relation (II.1) implique que $u_c = u_{ab} = u_a u_b$, ce qui est impossible car $u_c = 0$, $u_a \neq 0$ et $u_b \neq 0$. Étant donné que c est premier, nous allons le noter p.
(ii) Le sous-ensemble $F_p = \{u_0, u_1, \ldots, u_{p-1}\}$ de F est un sous-corps de F car il est isomorphe au corps $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$. En effet, il suffit de prendre l'application $f : F_p \to \mathbb{F}_p : u_i \mapsto i$.
(iii) Construisons l'ensemble $W_1 = \{u_0\omega_1, u_1\omega_1, \ldots, u_{p-1}\omega_1\} = \{u_i\omega_1 \mid u_i \in F_p\}$ à partir d'un élément $\omega_1 \in F \backslash F_p$. Cet ensemble possède p éléments. Si $q = p$, alors la thèse est démontrée. Sinon, nous construisons l'ensemble $W_2 = \{u_i\omega_1 + u_j\omega_2 \mid u_i, u_j \in F_p \text{ et } u_i \neq u_j\}$ à partir d'un élément $\omega_2 \in F \backslash W_1$. L'ensemble W_2 comporte p^2 éléments. Si $q = p^2$, alors la thèse est démontrée. Sinon, nous recommençons de même jusqu'à la construction de l'ensemble $W_m = \{u_i\omega_1 + u_j\omega_2 + \ldots + u_t\omega_m \mid u_i, u_j, \ldots, u_t \in F_p \text{ et } u_i \neq u_j \neq \cdots \neq u_t\}$ à partir d'un élément $\omega_m \in F \backslash W_{m-1}$. Cet ensemble comporte p^m éléments, ce qui termine la démonstration. □

Définition 26. Le nombre p défini dans le théorème 25 est appelé la *caractéristique* du corps F.

Remarque. Notons que dans un corps de caractéristique p, il est interdit de diviser par p. En effet, $pu_n = u_n + u_n + \cdots + u_n = u_{n+n+\cdots+n} = u_{pn} = u_p u_n = 0$.

II.3 Le corps fini $\mathbb{F}_q$ (avec $q = p^m$ et p premier)

II.3.1 Représentation

Le théorème 25 nous permet de voir le corps $\mathbb{F}_q$ comme un espace vectoriel sur $\mathbb{F}_p$. En effet, il suffit de prendre $\{\omega_1, \omega_2, \ldots, \omega_m\}$ comme base. Tout élément

u de $\mathbb{F}_q$ peut se mettre sous la forme unique

$$u = a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m, \tag{II.2}$$

avec $a_i \in \mathbb{F}_p \quad (i = 1, 2, \ldots, m)$. Nous représenterons donc les éléments de $\mathbb{F}_q$ par des m-uples $(a_1, a_2, \ldots, a_m)$.

Voyons à présent comment construire le corps $\mathbb{F}_q$.

Prenons pour domaine euclidien l'ensemble des polynômes à une variable à coefficients dans le corps fini $\mathbb{F}_p = \mathbb{Z} \bmod p$, i.e. $D = \mathbb{F}_p[x]$, avec p premier. Considérons un polynôme $f(x)$ de degré m, irréductible dans $\mathbb{F}_p$. Par le théorème 24, nous savons que $D \bmod f$ est un corps. Notons provisoirement ce corps $\mathbb{F}_q$. Comme $f(x)$ est de degré m, les éléments de $\mathbb{F}_q$ sont des polynômes de la forme

$$a_{m-1}x^{m-1} + a_{m-2}x^{m-2} + \cdots + a_1x + a_0, \tag{II.3}$$

avec $a_i \in \mathbb{F}_p \quad (i = 0, \ldots, m-1)$. Le corps $\mathbb{F}_q$ est donc fini, ce qui justifie la notation.

Nous retrouvons une représentation équivalente à (II.2).

Notation. Les éléments de $\mathbb{F}_{p^m}$ seront représentés comme un chaîne de chiffres en base p, c.-à-d. tout élément u de $\mathbb{F}_{p^m}$ sera noté $[u_{m-1}\, u_{m-2}\, \ldots\, u_1\, u_0]$. Cette notation est appelée *représentation en base polynomiale.*

II.3.2 Addition et multiplication

L'addition de deux éléments de $\mathbb{F}_q$ se fait simplement comme suit :

$$\begin{aligned}[a_{m-1}\, a_{m-2}\, \ldots\, a_1\, a_0] + [a'_{m-1}\, a'_{m-2}\, \ldots\, a'_1\, a'_0] = \\ [a_{m-1} + a'_{m-1}\ a_{m-2} + a'_{m-2}\ \ldots\ a_1 + a'_1\ a_0 + a'_0].\end{aligned}$$

Afin de bien comprendre comment se fait la multiplication, nous allons travailler sur un exemple. La procédure utilisée reste néanmoins la même quel que soit le corps $\mathbb{F}_q$ envisagé.

Exemple 14. Soient $p = 2$ et $f(x) = x^3 + x + 1$. Ce polynôme est irréductible sur $\mathbb{F}_2$ car $f(0) = f(1) = 1$, $f(x)$ n'a donc pas de zéros dans $\mathbb{F}_2$; et une cubique qui n'a pas de zéros dans un corps est irréductible sur ce corps. Comme $f(x)$ est de degré 3, les éléments de $\mathbb{F}_{2^3}$ sont de la forme $a_2x^2 + a_1x + a_0$ avec $a_i \in \mathbb{F}_2$ pour $i = 1, 2, 3$.

Multiplions deux éléments de $\mathbb{F}_{2^3}$:

$$\begin{aligned}(a_2x^2 + a_1x + a_0)(a_2'x^2 + a_1'x + a_0') \\ &= a_2a_2'x^4 + (a_2a_1' + a_1a_2')x^3 + (a_2a_0' + a_1a_1' + a_0a_2')x^2 + (a_1a_0' + a_0a_1')x \\ &\qquad + a_0a_0' \\ &= (a_2a_2' + a_2a_0' + a_1a_1' + a_0a_2')x^2 + (a_2a_2' + a_2a_1' + a_1a_2' \\ &\qquad + a_1a_0' + a_0a_1')x + a_2a_1' + a_1a_2' + a_0a_0'\end{aligned}$$

car

$$x^3 \equiv x + 1 \pmod{x^3 + x + 1}$$

et, par conséquent,

$$x^4 \equiv x^2 + x \pmod{x^3 + x + 1}.$$

Nous obtenons ainsi

$$[a_2\, a_1\, a_0] \cdot [a_2'\, a_1'\, a_0'] = [a_2a_2' + a_2a_0' + a_1a_1' + a_0a_2' \quad a_2a_2' + a_2a_1' + a_1a_2' + a_1a_0' + a_0a_1'\ a_2a_1' + a_1a_2' + a_0a_0'].$$

Par exemple, $[110] \cdot [111] = [342] = [100]$. Nous pouvons également calculer le produit de deux éléments en construisant une table de "logarithmes".

Calculons les puissances successives de x :

$$\begin{aligned}x^0 &= 1,\\ x^1 &= x,\\ x^2 &= x^2,\\ x^3 &= x + 1,\\ x^4 &= x^2 + x,\\ x^5 &= x^3 + x^2 = x^2 + x + 1,\\ x^6 &= x^3 + x^2 + x = x^2 + 1,\\ x^7 &= x^3 + x = 1.\end{aligned}$$

Par conséquent, $\alpha = [010]$ est un générateur du groupe multiplicatif $\mathbb{F}_{2^3}^*$ du corps $\mathbb{F}_{2^3}$. Tout élément non nul de $\mathbb{F}_{2^3}$ est donc une puissance de α. Si nous supposons que

$$\log_\alpha \beta = k \quad \text{signifie} \quad \alpha^k = \beta,$$

alors nous construisons la table suivante :

β	$\log_\alpha \beta$	k	α^k
[000]	–	–	[000]
[001]	0	0	[001]
[010]	1	1	[010]
[011]	3	2	[100]
[100]	2	3	[011]
[101]	6	4	[110]
[110]	4	5	[111]
[111]	5	6	[101]

Pour calculer $[110] \cdot [111]$, nous regardons dans la table les valeurs de $\log_\alpha[110] = 4$ et de $\log_\alpha[111] = 5$; donc $[110] \cdot [111] = \alpha^{4+5} = \alpha^7\alpha^2 = \alpha^2 = [100]$.

À retenir.

- Un *domaine euclidien* est un domaine intégral D muni d'une fonction de *mesure* $g : D \to \mathbb{N}$ telle que $\forall a, b \in D$:
  - $g(a) \leq g(ab)$ si $b \neq 0$,
  - $\exists q, r \in D : a = qb + r$ avec $r = 0$ ou $g(r) < g(b)$.
- Si D est un domaine euclidien et si p est premier dans D, alors $D \bmod p$ est un *corps*.
- La *cardinalité* d'un corps fini est une puissance d'un nombre premier, appelé *caractéristique* du corps.
- Le corps $\mathbb{F}_{p^m}$ peut être considéré comme un *espace vectoriel* sur $\mathbb{F}_p$; tout élément u de $\mathbb{F}_{p^m}$ est noté comme une chaîne de chiffres en base p, i.e. $u = [u_{m-1}u_{m-2}\ldots u_1u_0]$ avec $u_i \in \mathbb{F}_p$.

Partie III
Plan projectif et courbes planes

Résumé. Cette partie définira de plusieurs façons le plan projectif sur un corps. Ensuite, l'intersection de droites et de courbes du plan projectif sera analysée pour aboutir au théorème de Bezout.

III.1 Le plan projectif $\mathbb{P}_2$

Définition 27. Soit un corps K. Le *plan projectif* $\mathbb{P}_2(K)$ est l'ensemble des points $P = (a, b, c) \neq (0, 0, 0) \in K^3$ de sorte que deux points $P = (a, b, c)$ et $P' = (a', b', c')$ sont considérés comme étant des points équivalents s'il existe $t \in K^*$ tel que $(a, b, c) = t(a', b', c')$. Les nombres a, b et c sont appelés les *coordonnées homogènes* du point P.

Plus généralement, nous définissons le *n-espace projectif* $\mathbb{P}_n(K)$ comme l'ensemble des classes d'équivalence des $(n+1)$-uples suivants :

$$\mathbb{P}_n(K) = \frac{\{(a_0, a_1, \ldots, a_n) \in K^{n+1} \mid a_0, a_1, \ldots, a_n \text{ non tous nuls}\}}{\sim},$$

où $(a_0, a_1, \ldots, a_n) \sim (a'_0, a'_1, \ldots, a'_n)$ s'il existe $t \in K^*$ tel que

$$(a_0, a_1, \ldots, a_n) = t(a'_0, a'_1, \ldots, a'_n).$$

Définition 28. Soit un corps K. Le degré d'un terme d'un polynôme p de l'anneau $K[X_1, \ldots, X_n]$ est la somme des exposants des variables X_i apparaissant dans ce terme. Le *degré du polynôme* p est le plus grand degré de ses termes.

Exemple 15. Le polynôme $p(X, Y, Z) = 3X^3Y + 4X^2Y^2Z - YZ^2$ est un polynôme de degré 5.

Définition 29. Soit un corps K. Un polynôme $p \in K[X_1, \ldots, X_n]$ est un polynôme *homogène* de degré d si chacun de ses termes est de degré d. De plus, p est dit *irréductible* s'il ne peut pas s'écrire comme le produit non trivial de deux polynômes de $K[X_1, \ldots, X_n]$.

Notation. Si p est un polynôme homogène de degré d défini sur un corps K et à n variables, alors nous écrirons $p \in K[X_1, \ldots, X_n]_d$.

Proposition 30. *Soient un corps K et un polynôme non nul $p(X_1, \ldots, X_n)$ à coefficients dans K. Alors, p est est un polynôme homogène de degré $d > 0$ si et seulement si, pour une variable auxiliaire t,*

$$p(tX_1, \ldots, tX_n) = t^d p(X_1, \ldots, X_n). \tag{III.1}$$

Preuve. La condition nécessaire est évidente. Démontrons la condition suffisante. Écrivons p comme une somme de polynômes homogènes non nuls de degré d_i :

$$p = p_{d_1} + p_{d_2} + \cdots + p_{d_k}, \quad d_1 < d_2 < \cdots < d_k.$$

La relation (III.1) implique que

$$t^{d_1} p_{d_1} + t^{d_2} p_{d_2} + \cdots + t^{d_k} p_{d_k} = t^d p = t^d p_{d_1} + t^d p_{d_2} + \cdots + t^d p_{d_k},$$

et donc, $t^{d_i} = t^d$ pour tout i. Par conséquent, $k = 1$ car $d_1 < d_2 < \cdots < d_k$, et $p = p_{d_1} = p_d$. □

Corollaire 31 (Formule d'Euler). *Si $F \in K[X_1, \ldots, X_n]_d$ est un polynôme homogène de degré d défini sur un corps K, alors*

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i} = d \cdot F.$$

Preuve. La proposition 30 donne $F(tX_1, \ldots, tX_n) = t^d F(X_1, \ldots, X_n)$. En dérivant par rapport à t, il vient que

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i}(tX_1, \ldots, tX_n) = d t^{d-1} F(X_1, \ldots, X_n).$$

Si nous prenons $t = 1$ dans la relation précédente, nous obtenons la thèse. □

Remarque. La dérivée d'un polynôme se définit de manière purement algébrique. Si $p(X) = \sum_{k=0}^{n} a_k X^k$ est un polynôme de l'anneau $K[X]$, alors

$$\left(\sum_{k=0}^{n} a_k X^k \right)' = \sum_{k=1}^{n} a_k k X^{k-1}.$$

Définition 32. Soit un corps K. Une *courbe* C de $\mathbb{P}_2(K)$ est l'ensemble des points qui satisfait à

$$p(X, Y, Z) = 0,$$

où $p \in K[X, Y, Z]_d$ est un polynôme homogène de degré $d \geq 1$. Si $d = 1$, alors C est appelée une droite ; si $d = 2$, une conique ; si $d = 3$, une cubique, etc... Le nombre d est appelé le *degré* de la courbe.

Le plan usuel (x, y) sur un corps K, encore appelé *plan affine* et noté $\mathbb{A}_2(K)$, est l'ensemble des point $(x, y) \in K^2$. Si nous introduisons les coordonnés X, Y, Z telles que $x = X/Z$ et $y = Y/Z$, alors à tout point (x, y) de $\mathbb{A}_2(K)$ correspond le point (X, Y, Z) de $\mathbb{P}_2(K)$. Réciproquement, si $Z \neq 0$, alors à tout point (X, Y, Z) de $\mathbb{P}_2(K)$ correspond le point (x, y) de $\mathbb{A}_2(K)$. Voyons à présent ce qui se passe quand $Z = 0$. Considérons, dans $\mathbb{A}_2(K)$, deux droites parallèles $L : ax+by+c = 0$ et $L' : a'x+b'y+c = 0$ où $a' = ta$ et $b' = tb$. En coordonnées homogènes, c.-à-d. dans $\mathbb{P}_2(K)$, ces droites s'écrivent $L : aX + bY + cZ = 0$ et $L' : a'X + b'Y + c'Z = 0$. L'intersection de ces droites a lieu en un point pour lequel $Z = 0$. Un tel point est appelé *point à l'infini*. Cela permet de donner une nouvelle définition de $\mathbb{P}_2(K)$:

$$\mathbb{P}_2(K) = \mathbb{A}_2(K) \cup \{\text{l'ensemble des directions dans } \mathbb{A}_2(K)\}.$$

Nous voyons donc que l'introduction des coordonnées homogènes n'oblige plus à faire la distinction entre droites parallèles ou non : deux droites distinctes s'intersectent en un point unique comme le montre la proposition 34.

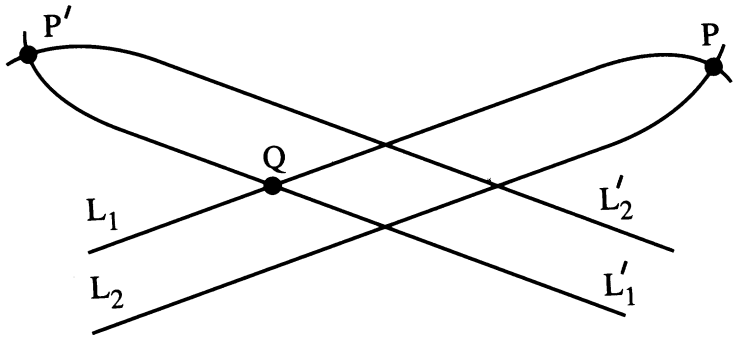


Figure 1: Intersection de droites parallèles.

Lemme 33 (Théorème du rang). *Soient V un espace vectoriel de dimension finie, W un espace vectoriel quelconque et $T : V \to W$ une application linéaire. Alors,*

$$\dim \operatorname{Ker} T + \dim \operatorname{Im} T = \dim V.$$

Preuve. Dans la suite, nous avons uniquement besoin du cas où W est de dimension finie ; nous allons donc uniquement démontrer le lemme avec cette hypothèse supplémentaire. Soient $\{v_1, \ldots, v_p\}$ et $\{w_1, \ldots, w_q\}$ des bases respectives de $\operatorname{Ker} T$ et de $\operatorname{Im} T$.
(i) Par définition de $\operatorname{Im} T$, $\exists y_i \in V$ tel que $T(y_i) = w_i$. Montrons que les

vecteurs $y_1, \ldots, y_q$ sont linéairement indépendants. Par l'absurde, si $\alpha_1 y_1 + \cdots + \alpha_q y_q = 0$, alors

$$T\left(\sum_{i=1}^{q} \alpha_i y_i\right) = \sum_{i=1}^{q} \alpha_i T(y_i) = \sum_{i=1}^{q} \alpha_i w_i = T(0) = 0.$$

Par conséquent, $w_1, \ldots, w_q$ sont linéairement dépendants et ne forment pas une base.
(ii) Montrons que $\{v_1, \ldots, v_p, y_1, \ldots, y_q\}$ est une base de V. L'indépendance linéaire de $v_1, \ldots, v_p, y_1, \ldots, y_q$ se démontre de la même façon que pour $y_1, \ldots, y_q$. Il reste à démontrer le caractère générateur de $v_1, \ldots, v_p, y_1, \ldots, y_q$, i.e. $\forall x \in V, \exists \alpha_i, \beta_i$ tels que $x = \sum_{i=1}^{p} \alpha_i v_1 + \sum_{i=1}^{q} \beta_i y_i$. Or, étant donné que $\{w_1, \ldots, w_q\}$ est une base de $\operatorname{Im} T$,

$$T(x) = \sum_{i=1}^{q} \beta_i w_i = \sum_{i=1}^{q} \beta_i T(y_i) = T\left(\sum_{i=1}^{q} \beta_i y_i\right),$$

et donc $x - \sum_{i=1}^{q} \beta_i y_i \in \operatorname{Ker} T$ et est une combinaison linéaire de $v_1, \ldots, v_p$; ce qui signifie que x est une combinaison linéaire de $v_1, \ldots, v_p, y_1, \ldots, y_q$. □

Proposition 34. *Soient un corps K et deux droites distinctes*

$$L : aX + bY + cZ = 0 \quad \textit{et} \quad L' : a'X + b'Y + c'Z = 0$$

de $\mathbb{P}_2(K)$. Alors L et L' ont un unique point d'intersection. De plus, deux points distincts de $\mathbb{P}_2(K)$ définissent une et une seule droite.

Preuve. (i) Considérons l'application linéaire

$$T : \mathbb{P}_2(K) \to \mathbb{P}_2(K), \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

alors, comme L et L' sont distinctes, le rang de la matrice des coefficients vaut 2, et donc le noyau est de dimension $(3 - 2) = 1$.
(ii) Soient $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ deux points distincts de L et l'application linéaire

$$T : \mathbb{P}_2(K) \to \mathbb{P}_2(K), \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Comme P_1 et P_2 sont distincts, la matrice des coordonnées des points est de rang 2, et donc le noyau est de dimension 1. □

Revenons à la définition de $\mathbb{P}_2(K)$. Toute droite de $\mathbb{A}_2(K)$ est parallèle à une droite passant par l'origine de la forme $L : ax = by$. Cependant, si $(a', b') = (ta, tb)$, alors la droite $L' : a'x = b'y$ est la même droite que L. Par conséquent, l'ensemble des directions de $\mathbb{A}_2(K)$ est donné par les points (a, b) de la droite projective $\mathbb{P}_1(K)$. Nous avons alors

$$\mathbb{P}_2(K) = \mathbb{A}_2(K) \cup \mathbb{P}_1(K).$$

III.2 Intersections et théorème de Bezout

III.2.1 Intersection d'une droite et d'une courbe

Étudions l'intersection d'une droite L et d'une courbe C de degré d dans $\mathbb{P}_2$ définies sur un corps K. Dans un premier temps, nous allons supposer que K est un corps de caractéristique nulle[†] ou de caractéristique $p > d$. Fixons les notations :

$$C : F(X, Y, Z) = 0.$$

Nous savons que deux points distincts définissent une droite. Soient $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ deux points distincts de la droite L, alors L peut se paramétriser sous la forme

$$L : \begin{cases} X = sa_1 + ta_2 \\ Y = sb_1 + tb_2 \\ Z = sc_1 + tc_2 \end{cases}.$$

Les points d'intersection de la droite et de la courbe sont donc donnés par

$$F(sa_1 + ta_2, sb_1 + tb_2, sc_1 + tc_2) = 0. \tag{III.2}$$

Le point d'intersection P_1 correspond à $s = 1$ et $t = 0$. Considérons cette fonction comme une fonction de t et notons-la $f(t)$. Le développement en série de Mac-Laurin donne

$$f(t) = f(0) + \frac{f'(0)}{1!}t + \frac{f''(o)}{2!}t^2 + \cdots + \frac{f^{(d)}}{d!}t^d.$$

Définition 35. Nous dirons que L intersecte C en P_1 avec un *ordre* m si $f^{(m)}(0) \neq 0$ et si $f^{(l)}(0) = 0$ pour $l < m$.

Notation. Si P est un point d'intersection d'ordre m entre une droite L et une courbe C, alors nous notons $I(P, L, C) = m$. Par convention, si $P \notin L \cap C$, alors $I(P, L, C) = 0$.

[†] Cela signifie que K est infini.

Supposons que P_1 soit un point d'ordre $m \geq 2$. Cela signifie que $f'(0) = 0$ et donc, par (III.2), que

$$\left.\frac{\partial F}{\partial X}\right|_{P_1} a_2 + \left.\frac{\partial F}{\partial Y}\right|_{P_1} b_2 + \left.\frac{\partial F}{\partial Z}\right|_{P_1} c_2 = 0. \qquad \text{(III.3)}$$

Définition 36. Un point P d'une courbe $C : F(X, Y, Z) = 0$ est dit *singulier* si

$$\left.\frac{\partial F}{\partial X}\right|_{P} = \left.\frac{\partial F}{\partial Y}\right|_{P} = \left.\frac{\partial F}{\partial Z}\right|_{P} = 0;$$

sinon P est dit *non singulier* ou *simple*. De plus, la courbe C est appelée *courbe non singulière* si tous ses points sont simples.

Supposons que P_1 soit un point non singulier. La relation (III.3) implique que le point $P_2 = (a_2, b_2, c_2)$ appartient à la droite

$$\left.\frac{\partial F}{\partial X}\right|_{P_1} X + \left.\frac{\partial F}{\partial Y}\right|_{P_1} Y + \left.\frac{\partial F}{\partial Z}\right|_{P_1} Z = 0. \qquad \text{(III.4)}$$

Par le corollaire 31, le point $P_1 = (a_1, b_1, c_1)$ appartient également à cette droite. La relation (III.4) définit la *tangente* à la courbe C au point (simple) P_1.

Si K est un corps de caractéristique $p \leq d$, alors la formule de Mac-Laurin n'est plus applicable. En gardant les mêmes notations que ci-dessus, nous pouvons écrire f comme un polynôme en T, i.e.

$$f(t) = k_0 + k_1 t + \cdots + k_d t^d.$$

La seule différence avec ce qui précède est que nous ne pouvons plus exprimer les coefficients k_i sous la forme $\frac{f^{(i)}(0)}{i!}$. Nous dirons que le point P_1 est un *point d'ordre* m si $k_m \neq 0$ et si $k_l = 0$ pour $l < m$; les autres définitions restant les mêmes.

Lemme 37. *Soient un point P, une droite L et deux courbes C_1 et C_2. Alors*

$$I(P, L, C_1 C_2) = I(P, L, C_1) + I(P, L, C_2).$$

Preuve. Trivial. □

Lemme 38. *Soient un point P, une droite L et deux courbes C_1 et C_2. Si C_1 et C_2 ont le même degré et si $C_1 + C_2 \neq 0$, alors*

$$I(P, L, C_1 + C_2) \geq \min\{I(P, L, C_1), I(P, L, C_2)\}.$$

Preuve. Trivial. □

Proposition 39. *Si $F(X,1,0)$ est un polynôme en X et si $L : Z = 0$ est la droite à l'infini, alors $I((r,1,0),L,F)$ est égal à la multiplicité de r comme racine de $F(X,1,0)$.*

Preuve. Soit la transformation linéaire

$$T : \mathbb{P}_2 \to \mathbb{P}_2, \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} 1 & -r & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

qui envoie le point $(r,1,0)$ en $(0,0,1)$ et dont l'inverse est donnée par

$$T^{-1} : \mathbb{P}_2 \to \mathbb{P}_2, \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} 1 & 0 & r \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Notons

$$\begin{aligned} f(X,Y) &= F(T^{-1}(X,Y,1)) = F(X+r,1,Y), \\ l(X,Y) &= L(T^{-1}(X,Y,1)) = Y. \end{aligned}$$

Donc, $l(X,Y)$ est de la forme $bX - aY$ avec $b = 0$ et $a = -1$ que nous pouvons paramétriser par $\phi(t) = \begin{pmatrix} at \\ bt \end{pmatrix} = \begin{pmatrix} -t \\ 0 \end{pmatrix}$ et

$$f(\phi(t)) = f(-t,0) = F(-t+r,1,0).$$

$I((r,1,0),L,F)$ est alors donné par l'ordre de la racine de $f(\phi(t))$ en $t = 0$, soit encore par l'ordre de la racine de $F(-t+r,1,0)$ en $t = 0$, ce qui est égal à la multiplicité de r comme racine de $F(X,1,0)$. □

III.2.2 Théorème de Bezout

Le théorème de Bezout apparaît sous plusieurs formes en géométrie algébrique. Nous allons uniquement présenter une version faible de ce théorème.

Définition 40. Soit un corps K. Le *résultant*, noté $R(f,g)$, de deux polynômes f et $g \in K[X]$ est le déterminant

$$R(f,g) = \left|\begin{array}{cccccccccc} a_n & a_{n-1} & \dots & \dots & a_1 & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \\ b_m & b_{m-1} & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\\a\\a\\a\\a\end{array}}\right\} m \text{ lignes} \\ \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\\a\\a\\a\\a\\a\\a\end{array}}\right\} n \text{ lignes} \end{array},$$

si

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad g(X) = \sum_{i=0}^{m} b_i X^i.$$

Lemme 41. *Soit un corps K. Deux polynômes f et $g \in K[X]$ ont un facteur non constant en commun si et seulement si il existe des polynômes non nuls ϕ et $\psi \in K[X]$ de degré respectivement strictement inférieur à celui de f et à celui de g tels que $\psi f = \phi g$.*

Preuve. ($\Rightarrow$) Si f et g ont un facteur commun h, alors $f = h\phi$, $g = h\psi$ et $\psi f = \phi g$.
($\Leftarrow$) Si $\psi f = \phi g$, alors tout facteur irréductible de g divise soit ψ, soit f. Or, comme le degré de ϕ est strictement inférieur à celui de g, au moins un des facteurs irréductibles de g divise f. □

Théorème 42. *Soit un corps K. Deux polynômes f et $g \in K[X]$ donnés par*

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad \textit{et} \quad g(X) = \sum_{i=0}^{m} b_i X^i$$

ont un facteur non constant en commun si et seulement si

$$R(f,g) = \left|\begin{array}{cccccccccc} a_n & a_{n-1} & \dots & \dots & a_1 & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \\ b_m & b_{m-1} & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \end{array}\right| = 0.$$

Preuve. ($\Rightarrow$) Par le lemme précédent, $\exists\phi$ et $\psi \in K[X]$ tels que $\psi f = \phi g$ où

$$\phi(X) = \sum_{i=0}^{n-1} \alpha_i X^i \quad \text{et} \quad \psi(X) = \sum_{i=0}^{m-1} \beta_i X^i$$

avec au moins un $\alpha_i \neq 0$ et un $\beta_i \neq 0$. Il s'ensuit que

$$\begin{array}{lll}
a_0\beta_0 & = b_0\alpha_0, & \\
a_1\beta_0 + a_0\beta_1 & = b_1\alpha_0 & + b_0\alpha_1, \\
a_2\beta_0 + a_1\beta_1 + a_0\beta_2 & = b_2\alpha_0 & + b_1\alpha_1 + b_0\alpha_2\ , \\
\vdots & \vdots & \\
a_n\beta_{m-1} = & & b_m\alpha_{n-1}.
\end{array}$$

Si nous considérons ce système comme un système homogène de $m+n$ équations à $m+n$ variables, nous avons une solution non triviale

$$(\beta_0, \ldots, \beta_{m-1}, \alpha_0, \ldots, \alpha_{n-1}).$$

Le déterminant du système est donc nul et par conséquent $R(f,g) = 0$.
($\Leftarrow$) Si $R(f,g) = 0$, alors il existe un α_i ou un β_i différent de 0. Si $\alpha_i \neq 0$, alors $\phi \neq 0$, et $\psi f = \phi g$ avec $\phi \neq 0$ et donc $\psi \neq 0$. □

Lemme 43. *Soit un corps K. Si F et $G \in K[X,Y,Z]$ sont deux courbes de degré respectif n et m vues comme des polynômes en l'unique variable Z à coefficients dans l'anneau $K[X,Y]$, alors le résultant de F et de G par rapport à Z, noté $R(X,Y)$, est soit nul, soit un polynôme homogène de degré mn.*

Preuve. Soient

$$\begin{aligned}
F(X,Y,Z) &= A_0(X,Y)Z^n + A_1(X,Y)Z^{n-1} + \cdots + A_n(X,Y), \\
G(X,Y,Z) &= B_0(X,Y)Z^m + B_1(X,Y)Z^{m-1} + \cdots + B_m(X,Y),
\end{aligned}$$

où $A_i(X,Y)$ et $B_i(X,Y)$ sont des polynômes homogènes de degré i. Alors,

$$R(tX,tY) = \begin{vmatrix}
A_0 & tA_1 & \ldots & t^nA_n & 0 & \ldots & 0 \\
0 & A_0 & tA_1 & \ldots & t^nA_n & & 0 \\
\vdots & & \ddots & \ddots & & \ddots & \vdots \\
0 & 0 & 0 & A_0 & tA_1(X,Y) & \ldots & t^nA_n \\
B_0 & tB_1 & \ldots & t^mB_m & 0 & \ldots & 0 \\
0 & B_0 & tB_1 & \ldots & t^mB_m & & 0 \\
\vdots & & \ddots & \ddots & & \ddots & \vdots \\
0 & 0 & 0 & B_0 & tB_1 & \ldots & t^mB_m
\end{vmatrix}.$$

Si nous multiplions la $i^{\text{ième}}$ ligne par t^{i-1} et la $(m+j)^{\text{ième}}$ ligne par t^{j-1}, nous obtenons

$$\begin{aligned} t^\alpha R(tX,tY) &= \begin{vmatrix} A_0 & tA_1 & \dots & t^nA_n & 0 & \dots & 0 \\ 0 & tA_0 & t^2A_1 & \dots & t^{n+1}A_n & & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & t^{m-1}A_0 & t^mA_1(X,Y) & \dots & t^{n+m-1}A_n \\ B_0 & tB_1 & \dots & t^mB_m & 0 & \dots & 0 \\ 0 & tB_0 & t^2B_1 & \dots & t^{m+1}B_m & & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & t^{n-1}B_0 & t^nB_1 & \dots & t^{m+n-1}B_m \end{vmatrix} \\ &= t^\beta R(X,Y), \end{aligned}$$

où la deuxième égalité est obtenue en mettant t^i en évidence dans la $(i+1)^{\text{ième}}$ colonne. Nous avons donc

$$\alpha = (1+2+\cdots+(m-1)) + (1+2+\cdots+(n-1)) = \frac{(m-1)m}{2} + \frac{(n-1)n}{2}$$

et

$$\beta = 1+2+\cdots+(m+n-1) = \frac{(m+n-1)(m+n)}{2}.$$

Comme $\beta - \alpha = mn$, $R(tX,tY) = t^{mn}R(X,Y)$, et donc, par la proposition 30, $R(X,Y)$ est soit un polynôme de degré mn, soit un polynôme nul. □

Théorème 44 (Théorème faible de Bezout). *Soit un corps infini K. Si $F \in K[X,Y,Z]_m$ et $G \in K[X,Y,Z]_n$ sont deux courbes ayant plus de mn points communs, alors F et G ont un facteur non constant en commun.*

Preuve. Les courbes F et G ont au moins $mn+1$ points en commun ; joignons chaque paire de points par une droite. Comme le nombre de droites est fini et que K est infini, il existe un point P qui n'appartient à aucune de ces droites, ni à F, ni à G. Choisissons un système de coordonnées homogènes tel que $P = (0,0,1)$. Nous pouvons considérer F et G comme des polynômes en Z :

$$\begin{aligned} F(X,Y,Z) &= A_0(X,Y)Z^m + A_1(X,Y)Z^{m-1} + \cdots + A_m(X,Y), \\ G(X,Y,Z) &= B_0(X,Y)Z^n + B_1(X,Y)Z^{n-1} + \cdots + B_n(X,Y), \end{aligned}$$

où $A_i(X,Y)$ et $B_i(X,Y)$ sont des polynômes homogènes de degré i. Par le lemme 43, le résultant de F et de G par rapport à Z, i.e. $R(X,Y)$, est soit un polynôme nul, soit un polynôme de degré mn. Notons (a,b,c) un des

$mn + 1$ points d'intersection. Ce point appartient à $F \cap G$, ce qui signifie que $F(a, b, Z)$ et $G(a, b, Z)$ ont une racine commune c. Par conséquent, $R(a, b) = 0$. Comme aucun des couples (a, b) correspondant aux $mn + 1$ points d'intersection ne sont proportionnels (car ils ne sont pas colinéaires à $P = (0, 0, 1)$), $R(X, Y)$ ne peut pas être de degré mn. Il vient donc que $R(X, Y) = 0$ et, par le théorème 42, F et G ont un facteur non constant en commun. □

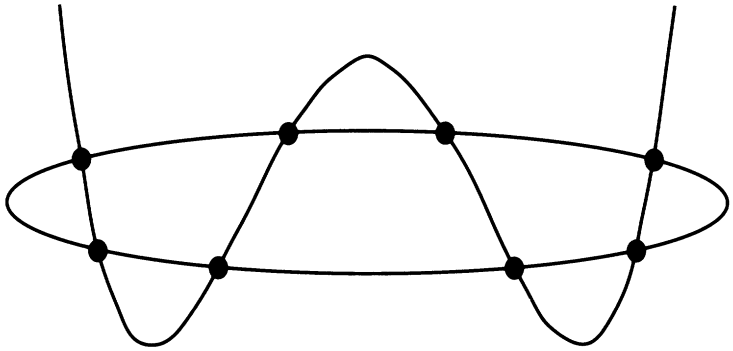


Figure 2: Intersection d'une courbe de degré 4 et d'une courbe de degré 2.

Corollaire 45. *Soit un corps infini K. Si $C \in K[X, Y.Z]_d$ est une courbe et si L est une droite telle que $\sum_{P \in L} I(P, L, C) > d$, alors L divise C.*

Preuve. Par l'absurde, supposons que L ne divise pas C. Par le théorème 44, nous savons que C et L ont un nombre fini de points communs et, par conséquent, $\sum_{P \in L}(I, L, C)$ est fini. Montrons que $\sum_{P \in L} I(P, L, C) \leq d$. Par une transformation projective, nous pouvons supposer que L est la droite à l'infini $Z = 0$. En faisant éventuellement une translation sur la variable Y, nous pouvons également supposer que tous les points d'intersection ont une coordonnée en Y non nulle. Notons $P_i = (r_i, 1, 0)$ les points d'intersection de $C(X, 1, 0)$ avec $L : Z = 0$. Comme K est infini, il existe $(r, 1, 0)$ qui n'appartient pas à $C \cap L$ et donc, $C(X, 1, 0)$ est un polynôme non nul. Ce polynôme a donc au plus d racines comptées avec leur mutiplicité. Par conséquent, par la proposition 39, $\sum_{P \in L} I(P, L, C) \leq d$, ce qui est contraire à l'hypothèse. □

À retenir.

▶ Soit un corps K. Le *n-espace projectif* $\mathbb{P}_n(K)$ est l'ensemble des classes d'équivalence des $(n+1)$-uples

$$\mathbb{P}(K) = \frac{\{(a_0, a_1, \ldots, a_n) \mid a_0, a_1, \ldots, a_n \text{ non tous nuls}\}}{\sim},$$

où $(a_0, a_1, \ldots, a_n) \sim (a'_0, a'_1, \ldots, a'_n)$ si

$$(a_0, a_1, \ldots, a_n) = t(a_0, a_1, \ldots, a_n)$$

avec $t \in K\backslash\{0\}$. Si $n = 2$, alors $\mathbb{P}_2(K)$ est le *plan projectif*.

▶ Une *courbe* de $\mathbb{P}_2(K)$ est un polynôme homogène de degré $d \geq 1$ de l'anneau $K[X, Y, Z]$. Si $d = 1$, alors c'est une droite ; si $d = 2$, une conique ; si $d = 3$, une cubique.

▶ Un point P d'une courbe $C : F(X, Y, Z) = 0$ est un *point singulier* si

$$\left.\frac{\partial F}{\partial X}\right|_P = \left.\frac{\partial F}{\partial Y}\right|_P = \left.\frac{\partial F}{\partial Z}\right|_P = 0.$$

Une courbe dont tous les points sont non singuliers est une *courbe non singulière*.

▶ Une courbe est *irréductible* si elle ne peut pas s'écrire comme le produit non trivial de deux polynômes.

Partie IV
Courbes elliptiques

Résumé. Cette partie est le coeur de ce rapport. Elle définira ce qu'est une courbe elliptique et le groupe topologique d'une telle courbe. Il sera également montré qu'une courbe elliptique peut s'écrire sous une forme particulière appelée "équations de Weierstrass".

IV.1 Définition

Définition 46. Une *courbe elliptique* est une paire $(E, \mathcal{O})$, où E est une cubique irréductible non singulière et $\mathcal{O} \in E$. La courbe elliptique E est *définie sur un corps* K si E est une courbe sur K et si $\mathcal{O} \in E(K)$.

IV.2 Équations de Weierstrass

Théorème 47. *Si E est une courbe elliptique définie sur un corps K, alors il existe une application*

$$\phi : E(K) \to \mathbb{P}^2(K)$$

qui fournit un isomorphisme de $E(K)$ sur une courbe $C(K)$ donnée par l'équation de Weierstrass

$$C : F(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

où $a_1, \ldots, a_6 \in K$; et tel que $\phi(\mathcal{O}) = (0,1,0)$.

Preuve. Voir section IV.3. □

Pour alléger les notations, nous allons écrire l'équation de Weierstrass en coordonnées non homogènes : $x = X/Z$ et $y = Y/Z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{IV.1}$$

plus le point à l'infini $\mathcal{O} = (0,1,0)$. Remarquons que $\mathcal{O}$ est le seul point à l'infini et qu'il n'est pas singulier car $(\partial F/\partial Z)(0,1,0) = 1 \neq 0$. Nous définissons également les quantités suivantes :

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$
$$c_4 = b_2^2 - 24b_4 \quad \text{et} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

Définition 48. Le *discriminant* Δ de l'équation de Weierstrass est la quantité

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \tag{IV.2}$$

et le *j-invariant* de la courbe elliptique E est la quantité

$$j(E) = \frac{c_4^3}{\Delta}. \tag{IV.3}$$

Corollaire 49. *Soit un corps K de caractéristique p. Une courbe E définie sur K donnée par une équation de Weierstrass prend alors une forme simplifiée,*

1. *si $p \neq 2$ et $p \neq 3$,*

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2),$$
$$j(E) = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}; \tag{IV.4}$$

2. *si $p = 2$ et si $j(E) \neq 0$,*

$$y^2 + xy = x^3 + a_2 x^2 + a_6, \quad \Delta = a_6, \quad j(E) = 1/a_6; \tag{IV.5}$$

si $p = 2$ et si $j(E) = 0$,

$$y^2 + a_3 y = x^3 + a_4 x + a_6, \quad \Delta = a_3^4, \quad j(E) = 0; \tag{IV.6}$$

3. *si $p = 3$ et si $j(E) \neq 0$,*

$$y^2 = x^3 + a_2 x^2 + a_6, \quad \Delta = -a_2^3 a_6, \quad j(E) = -a_2^3/a_6; \tag{IV.7}$$

si $p = 3$ et si $j(E) = 0$,

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j(E) = 0. \tag{IV.8}$$

Preuve. (i) Si $p \neq 2$, nous pouvons remplaçer y par $(y - \frac{1}{2}(a_1 x + a_3))$. Nous obtenons alors $y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$. De surcroît, si $p \neq 3$, alors nous remplaçons x par $(x - \frac{b_2}{12})$ pour obtenir $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$.
(ii) L'invariant (en caractéristique 2) de l'équation générale de Weierstrass $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ vaut $j(E) = a_1^{12}/\Delta$. Si $j(E) = 0$, et donc si $a_1 = 0$, alors la substitution $x \leftarrow (x+a_2)$ donne $y^2+a_3y = x^3+(a_2^2+a_4)x+(a_2^3+a_4a_2+a_6)$; sinon, nous remplaçons (x, y) par $((a_1^2x + \frac{a_3}{a_1}), a_1^3 y + \frac{a_1^2 a_4 + a_3^2}{a_1^3})$ pour avoir $y^2 + xy = x^3 + \frac{a_1 a_2 + a_3}{a_1^3}x^2 + \frac{a_1^4 a_2^2 + a_3^4 + a_1^5 a_3 a_4 + a_1^3 a_3^3 + a_1^4 a_2 a_3^2 + a_1^6 a_6}{a_1^{12}}$.
(iii) En (i), nous avons montré que si $p \neq 2$, alors $y^2 = x^3 + a_2x^2 + a_4x + a_6$. L'invariant de cette courbe (en caractéristique 3) vaut $j(E) = a_2^2/\Delta$. Si $j(E) = 0$, alors $a_2 = 0$ et nous avons l'expression demandée ; sinon il suffit de remplaçer x par $(x + \frac{a_4}{a_2})$ pour obtenir $y^2 = x^3 + a_2x^2 + \frac{2a_2^2a_4^2 + a_2^3a_6 + a_4^3}{a_2^3}$. □

Lemme 50. *Soit un corps K et une courbe E donnée par l'équation de Weierstrass :*

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

dont le discriminant vaut Δ et le j-invariant, $j(E)$. Le changement de variables

$$(x,y) \leftarrow (u^2x + r, u^3y + u^2sx + t) \quad \textit{avec } r,s,t,u(\neq 0) \in K \tag{IV.9}$$

transforme l'équation précédente en

$$E' : f'(x,y) = y^2 + a_1'xy + a_3'y - x^3 - a_2'x^2 - a_4'x - a_6' = 0,$$

où les coefficients sont donnés par

$$\begin{aligned} ua_1' &= a_1 + 2s, \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2, \\ u^3a_3' &= a_3 + ra_1 + 2t, \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st. \end{aligned}$$

De plus, $u^{12}\Delta' = \Delta$ et $j(E') = j(E)$.

Preuve. Il suffit de remplaçer x et y par leurs nouvelles expressions pour obtenir les relations désirées. □

Il est à noter que toutes les transformations effectuées dans la démonstration du corollaire 49 sont de la forme (IV.9).

Théorème 51. *Soit K un corps de caractéristique p. Deux courbes données par leur équation de Weierstrass dont le discriminant est non nul sont isomorphes si et seulement si elles sont le même j-invariant.*

Preuve. ($\Rightarrow$) Par le lemme précédent.
($\Leftarrow$) Pour simplifier les calculs, nous allons supposer que $p \neq 2, 3$. Soient deux courbes E et E' ayant le même j-invariant dont les équations de Weierstrass sont données par

$$\begin{aligned} E &: y^2 = x^3 + a_4x + a_6, \\ E' &: y'^2 = x^3 + a_4'x + a_6'. \end{aligned}$$

Comme $j(E) = 1728\frac{4a_4^3}{4a_4^3+27a_6^2}$ et $j(E') = 1728\frac{4a_4'^3}{4a_4'^3+27a_6'^2}$ sont égaux, cela implique que $a_6^2a_4'^3 = a_4^3a_6'^2$. Cherchons des isomorphismes de la forme $(x,y) \leftarrow$

(u^2x, u^3y).
1° Si $a_4 = 0$, alors $a_6 \neq 0$ (car $\Delta \neq 0$) et donc $a'_4 = 0$. Nous obtenons un isomorphisme en prenant $u = (a_6/a'_6)^{1/6}$.
2° Si $a_6 = 0$, alors $a_4 \neq 0$ (car $\Delta \neq 0$) et donc $a'_6 = 0$. Nous obtenons un isomorphisme en prenant $u = (a_4/a'_4)^{1/4}$.
3° Si $a_4 a_6 \neq 0$, alors $a'_4 a'_6 \neq 0$. Nous obtenons un isomorphisme en prenant $u = (a_4/a'_4)^{1/6} = (a_6/a'_6)^{1/4}$.
Si $p = 2$ ou 3, la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Théorème 52. *Soit E une courbe donnée par une équation de Weierstrass. Alors E est non singulière si et seulement si $\Delta \neq 0$.*

Preuve. ($\Leftarrow$) Soit l'équation générale de Weierstrass :

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0.$$

Montrons d'abord que le point à l'infini $\mathcal{O} = (0, 1, 0)$ n'est jamais singulier. Regardons E comme une courbe de $\mathbb{P}^2$:

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Comme $(\partial F/\partial Z)(\mathcal{O}) = 1 \neq 0$, $\mathcal{O}$ n'est pas un point singulier de E. Par l'absurde, supposons que E soit singulière en un point $P_0 = (x_0, y_0)$. Par le changement de variables $(x, y) \leftarrow (x - x_0, y - y_0)$, nous ramenons le point P_0 en $(0, 0)$. Par le lemme 50, cette transformation ne modifie pas le discriminant (car $u = 1$). Nous avons alors $a_6 = f(0, 0) = 0$, $a_4 = (\partial f/\partial x)(0, 0) = 0$ et $a_3 = (\partial f/\partial y)(0, 0) = 0$. La courbe E a donc pour équation :

$$E : f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = 0.$$

Le discriminant de cette équation est nul, ce qui contredit l'hypothèse.
($\Rightarrow$) Pour simplifier les calculs, nous allons supposer que $p \neq 2, 3$. Soit alors la courbe E donnée par l'équation de Weierstrass :

$$E : y^2 = x^3 + a_4x + a_6.$$

Si la courbe est singulière en un point $P_0 = (x_0, y_0)$, alors

$$2y_0 = 0 \Rightarrow y_0 = 0,$$
$$3x_0^2 + a_4 = 0 \Rightarrow x_0^2 = -\frac{a_4}{3}.$$

Or $P_0 = (x_0, y_0)$ est un point de la courbe, par conséquent, $y_0^2 = 0 = x_0^3 + a_4x_0 + a_6 = \frac{2}{3}a_4x_0 + a_6$. Il s'ensuit que $x_0^2 = \frac{9a_6^2}{4a_4^2} = -\frac{a_4}{3}$ et donc $\Delta = -16(4a_4^3 + 27a_6^2) = 0$. Si $p = 2$ ou 3, la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Les théorèmes 47, 51 et 52 permettent de donner une définition alternative d'une courbe elliptique.

Définition 53. Une *courbe elliptique* est une courbe isomorphe à la courbe donnée par une des équations de Weierstrass (IV.4) à (IV.8) où $\Delta \neq 0$ plus le point à l'infini $\mathcal{O} = (0, 1, 0)$.

IV.3 Réduction d'une cubique

Soit un corps K de caractéristique différente de 2. L'équation projective d'une cubique irréductible non singulière est donnée par $f(U, V, W) = 0$ où

$$f(U,V,W) = s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + (s_5U^2 + s_6UV + s_7V^2)W + (s_8U + s_9V)W^2 + s_{10}W^3. \quad \text{(IV.10)}$$

L'équation (IV.10) peut également être vue comme un polynôme de degré 3 en W :

$$f(U,V,W) = c_0W^3 + c_1(U,V)W^2 + c_2(U,V)W + c_3(U,V). \quad \text{(IV.11)}$$

Soit $P_0 = (u_0, v_0, w_0)$ un point de la courbe. La tangente en P_0 intersecte la courbe en un troisième point unique $P_1 = (u_1, v_1, w_1)$. Cette tangente a pour équation

$$\frac{\partial f}{\partial U}(u_0,v_0,w_0)U + \frac{\partial f}{\partial V}(u_0,v_0,w_0)V + \frac{\partial f}{\partial W}(u_0,v_0,w_0)W = 0. \quad \text{(IV.12)}$$

Sans perdre de généralités, nous pouvons supposer que $w_1 \neq 0$ (nous pouvons toujours nous ramener à cette situation en permutant éventuellement W avec U ou avec V). Faisons le changement de variables $(U, V, W) \leftarrow (U - u_1, V - v_1, Z)$. Le point P_1 a maintenant pour coordonnées $(0, 0, 1)$. Étant donné que ce point appartient à la tangente, la dérivée partielle de f par rapport à W en P_0 est nulle. Comme la courbe est non singulière, les dérivées partielles par rapport à U et à V en P_0 ne peuvent pas s'annuler simultanément. Pour fixer les idées, supposons que la dérivée partielle par rapport à V en P_0 soit non nulle (si cette dernière est nulle, nous permutons les variables U et V). Le point $P_1 = (0, 0, 1)$ appartient aussi à la courbe et donc $s_{10} = 0$.

Après changement de variables, les équations (IV.10), (IV.11) et (IV.12) deviennent :

$$f(U,V,W) = s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + (s_5U^2 + s_6UV + s_7V^2)W + (s_8U + s_9V)W^2, \quad \text{(IV.13)}$$

$$f(U,V,W) = c_1(U,V)W^2 + c_2(U,V)W + c_3(U,V), \tag{IV.14}$$

$$V = \lambda U \quad \text{où } \lambda = \frac{\frac{\partial f}{\partial U}\Big|_{P_0}}{\frac{\partial f}{\partial V}\Big|_{P_0}}, \tag{IV.15}$$

de plus, $P_0 = (u_0 - u_1, v_0 - v_1, w_0)$ et $P_1 = (0,0,1)$.

Théorème 54. *Avec les notations précédentes et nos hypothèses de travail, si nous notons*

$$d(U,V) = c_2^2(U,V) - 4c_1(U,V)c_3(U,V)$$

et

$$d(U, \lambda U + 1) = AU^4 + BU^3 + CU^2 + DU + E,$$

et si P_0 n'est pas un point à l'infini, i.e. $w_0 \neq 0$, alors

1. *$A = 0$ et $B \neq 0$;*
2. *la transformation*

$$X = \frac{BU}{V - \lambda U},$$
$$Y = \frac{B}{(V - \lambda U)^2}(2c_3(U,V) + c_2(U,V))$$

est une transformation birationnelle dont l'inverse est donnée par

$$U = X\frac{BY - c_2(X, \lambda X + B)}{2c_3(X, \lambda X + B)},$$
$$V = (\lambda X + B)\frac{BY - c_2(X, \lambda X + B)}{2c_3(X, \lambda X + B)};$$

3. *l'application birationnelle précédente transforme l'équation de la cubique en l'équation de Weierstrass*

$$Y^2 = X^3 + CX^2 + BDX + B^2E.$$

Preuve. (i) Si nous calculons $d(1,\lambda)$ et $\frac{\partial d}{\partial V}(1,\lambda)$, nous obtenons

$$d(1,\lambda) = (s_5 + s_6\lambda + s_7^2\lambda^2)^2 - 4(s_8 + s_9\lambda)(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)$$

et

$$\begin{aligned}\frac{\partial d}{\partial V}(1,\lambda) &= 2c_2(1,\lambda)\frac{\partial c_2}{\partial V}(1,\lambda) - 4c_1(1,\lambda)\frac{\partial c_3}{\partial V}(1,\lambda) - 4\frac{\partial c_1}{\partial V}(1,\lambda)c_3(1,\lambda)\\ &= 2(s_5 + s_6\lambda + s_7\lambda^2)(s_6 + 2s_7\lambda) - 4(s_8 + s_9\lambda)(s_2 + 2s_3\lambda + 3s_4\lambda^2)\\ &\quad -4s_9(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)\end{aligned}$$

Développons ensuite $d(U, \lambda U + 1)$:

$$\begin{aligned}
&d(U, \lambda U + 1) \\
&\quad = c_2^2(U, \lambda U + 1) - 4c_1(U, \lambda U + 1)c_3(U, \lambda U + 1) \\
&\quad = [(s_5 + s_6\lambda + s_7\lambda^2)U^2 + (s_6 + 2s_7\lambda)U + s_7]^2 - \\
&\qquad 4[(s_8 + s_9\lambda)U + s_9] \cdot [(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)U^3 + \\
&\qquad\quad (s_2 + 2s_3\lambda + 3s_4\lambda^2)U^2 + (s_3 + 3s_4\lambda)U + s_4] \\
&\quad = [(s_5 + s_6\lambda + s_7\lambda^2)^2 - 4(s_8 + s_9\lambda)(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)]U^4 + \\
&\qquad [2(s_5 + s_6\lambda + s_7\lambda^2)(s_6 + 2s_7\lambda) - 4(s_8 + s_9\lambda)(s_2 + 2s_3\lambda + 3s_4\lambda^2) \\
&\qquad\quad -4s_9(s_1 + s_2\lambda + s_3\lambda^2 + s_4\lambda^3)]U^3 + [\cdots]U^2 + [\cdots]U + [\cdots] \\
&\quad = d(1, \lambda)U^4 + \frac{\partial d}{\partial V}(1, \lambda)U^3 + [\cdots]U^2 + [\cdots]U + [\cdots].
\end{aligned}$$

Le point P_0 est un point de la tangente, il a donc pour coordonnées $(\alpha, \lambda\alpha, 1)$ avec $\alpha \neq 0$ car $P_0 \neq P_1$. Le point P_0 est une racine double de f. En résolvant par rapport à U dans (IV.14), nous avons $c_1(\alpha, \lambda\alpha) + c_2(\alpha, \lambda\alpha) + c_3(\alpha, \lambda\alpha) = \alpha[c_1(1, \lambda) + \alpha c_2(1, \lambda) + \alpha^2 c_3(1, \lambda)] = 0$; $\alpha = 0$ correspond à P_1 et $c_1(1, \lambda) + \alpha c_2(1, \lambda) + \alpha^2 c_3(1, \lambda) = 0$ correspond à la valeur double en P_0. Cette racine étant double, il s'ensuit que le discriminant est nul, i.e. $d(1, \lambda) = 0$ et que $c_3(1, \lambda) \neq 0$. Nous trouvons

$$\alpha = -\frac{c_2(1, \lambda)}{2c_3(1, \lambda)}.$$

Comme $d(1, \lambda) = 0$, nous avons démontré que $A = 0$. Il reste à montrer que $B \neq 0$. Calculons :

$$\begin{aligned}
&\frac{\partial f}{\partial V}(\alpha, \lambda\alpha, 1) \\
&\quad = \frac{\partial c_1}{\partial V}(\alpha, \lambda\alpha) + \frac{\partial c_2}{\partial V}(\alpha, \lambda\alpha) + \frac{\partial c_3}{\partial V}(\alpha, \lambda\alpha) \\
&\quad = \frac{\partial c_1}{\partial V}(1, \lambda) + \alpha\frac{\partial c_2}{\partial V}(1, \lambda) + \alpha^2\frac{\partial c_3}{\partial V}(1, \lambda) \\
&\quad = \frac{4c_3^2(1, \lambda)\frac{\partial c_1}{\partial V}(1, \lambda) - 2c_2(1, \lambda)c_3(1, \lambda)\frac{\partial c_2}{\partial V}(1, \lambda) + c_2^2(1, \lambda)\frac{\partial c_3}{\partial V}(1, \lambda)}{4c_3^2(1, \lambda)} \\
&\qquad\qquad \text{car } \alpha = -\frac{c_2(1, \lambda)}{2c_3(1, \lambda)} \\
&\quad = -\frac{-4c_3(1, \lambda)\frac{\partial c_1}{\partial V}(1, \lambda) + 2c_2(1, \lambda)\frac{\partial c_2}{\partial V}(1, \lambda) - 4c_1(1, \lambda)\frac{\partial c_3}{\partial V}(1, \lambda)}{4c_3(1, \lambda)} \\
&\qquad\qquad \text{car } A = d(1, \lambda) = c_2^2(1, \lambda) - 4c_1(1, \lambda)c_3(1, \lambda) = 0 \\
&\quad = -\frac{\frac{\partial d}{\partial V}(1, \lambda)}{4c_3(1, \lambda)} = -\frac{B}{4c_3(1, \lambda)} \neq 0
\end{aligned}$$

car la dérivée partielle par rapport à V en P_0 est non nulle par hypothèse.
(ii) Par substitution, nous voyons que si $B \neq 0$, les applications $(U,V) \to (X,Y)$ et $(X,Y) \to (U,V)$ sont les inverses l'une de l'autre.
(iii) En remplaçant U et V par leurs expressions respectives, nous obtenons

$$B^2Y^2 = d(X, \lambda X + B).$$

Or, comme $d(U,V)$ est un polynôme homogène de degré 4, nous voyons immédiatement que

$$d(X, \lambda X + B) = B(BX^3) + C(B^2X^2) + D(B^3X) + E(B^4).$$

Pour s'en convaincre, il suffit de regarder le développement de $d(U, \lambda U + 1)$ (voir p. 34). Nous avons finalement

$$B^2Y^2 = B^2(X^3 + CX^2 + DBX + EB^2),$$

ce qui termine la démonstration. □

IV.4 Loi de groupe

IV.4.1 Règle de la "sécante-tangente"

Proposition 55. *Soient une cubique irréductible non singulière C et une droite L définies sur un corps K. Si la cubique C a deux points d'intersection (comptés avec leur multiplicité) avec la droite L, alors C a trois points d'intersection (comptés avec leur multiplicité) avec la droite L.*

Preuve. Comme C est irréductible, $C \cap L$ a un nombre fini de points. Soit la droite $L : aX + bY + cZ = 0$ où, par symétrie, nous supposons $c \neq 0$. Les points d'intersection de C et de L sont les racines du polynôme

$$q(X,Y) = p(X, Y, -\frac{aX + bY}{c}) \in K[X,Y]_3.$$

Notons $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ (avec éventuellement $P_1 = P_2$), deux points d'intersection de C avec L, alors, comme $q(a_1, b_1) = q(a_2, b_2) = 0$, il vient que

$$q(X,Y) = v(X,Y) \prod_{i=1}^{2} (b_iX - a_iY) \quad \text{où } v(X,Y) \in K[X,Y]_1.$$

Le troisième point d'intersection de C avec L est alors donné par

$$P_3 = (a_3, b_3, -\frac{aa_3 + bb_3}{c})$$

où (a_3, b_3) est l'unique racine de $v(X,Y)$. □

Cette proposition permet de définir la *loi de composition de la sécante-tangente* :

1. Si $P, Q \in C(K)$ et si $P \neq Q$, alors nous définissons $L = PQ$, la droite sécante qui passe par P et Q. Par la proposition précédente, nous savons qu'il existe un troisième point unique (en comptant les multiplicités) qui appartient à $C \cap L$, nous notons ce troisième point $P * Q$.

2. Si $P \in C(K)$, alors nous définissons $L = PP$, la droite tangente à C qui passe par P. Par la proposition précédente, nous savons qu'il existe un troisième point unique (en comptant les multiplicités) qui appartient à $C \cap L$, nous notons ce troisième point $P * P$.

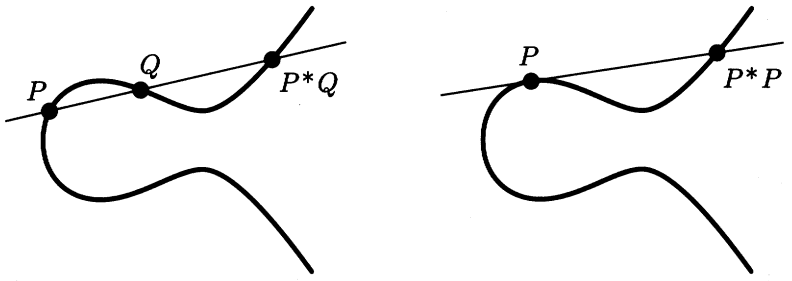


Figure 3: Règle de la sécante-tangente.

Proposition 56. *Soient un corps infini K et une cubique irréductible non singulière C. Pour tous points P_1, P_2, Q_1 et $Q_2 \in C(K)$, nous avons*

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2). \tag{IV.16}$$

Preuve. Construisons les matrices

$$M = \begin{pmatrix} P_1 & P_2 & P_1 * P_2 \\ Q_1 & Q_2 & Q_1 * Q_2 \\ P_1 * Q_1 & P_2 * Q_2 & (P_1 * Q_1) * (P_2 * Q_2) \end{pmatrix}$$

et

$$\widetilde{M} = \begin{pmatrix} P_1 & Q_1 & P_1 * Q_1 \\ P_2 & Q_2 & P_2 * Q_2 \\ P_1 * P_2 & Q_1 * Q_2 & (P_1 * P_2) * (Q_1 * Q_2) \end{pmatrix},$$

où les éléments de la ligne i de M (respectivement $\widetilde{M}$) sont des points de $C(K)$ de la droite L_i (respectivement $\widetilde{L}_i$) passant par ces éléments. Nous

devons montrer que $M = \widetilde{M}^t$.
(i) Considérons d'abord le cas où L_i et $\widetilde{L}_j$ ont uniquement un point d'intersection (c'est ce que nous appellerons l'hypothèse de travail (i)).
Posons $L = L_1L_2L_3$ et $\widetilde{L} = \widetilde{L}_1\widetilde{L}_2\widetilde{L}_3$. Choisissons ensuite a_1, a_2 et a_3 non tous nuls tels que

$$\begin{cases} a_1C(R_1) + a_2L(R_1) + a_3\widetilde{L}(R_1) = 0 \\ a_1C(R_2) + a_2L(R_2) + a_3\widetilde{L}(R_2) = 0 \end{cases}, \tag{IV.17}$$

avec $R_1(\neq P_1, P_2 \text{ et } P_1 * P_2) \in L_1$ et $R_2 \notin L$. Remarquons que R_1 et R_2 existent car K est infini. Construisons la cubique

$$C_0 = a_1C + a_2L + a_3\widetilde{L}.$$

a) Par l'absurde, supposons que $C_0 \neq 0$.

(1) Notons M_{1j} un élément quelconque de la première ligne de la matrice M. Par le lemme 37,

$$\begin{aligned} I(M_{1j}, L_1, \widetilde{L}) &= I(M_{1j}, L_1, \widetilde{L}_1) + I(M_{1j}, L_1, \widetilde{L}_2) + I(M_{1j}, L_1, \widetilde{L}_3) \\ &\geq 1. \end{aligned}$$

Or, par le lemme 38,

$$\begin{aligned} I(M_{1j}, L_1, C_0) &\geq \min\{I(M_{1j}, L_1, C), I(M_{1j}, L_1, L), I(M_{1j}, L_1, \widetilde{L})\} \\ &\geq 1. \end{aligned}$$

Par (IV.17), R_1 est un point de C_0 et donc $I(R_1, L_1, C_0) \geq 1$ car $R_1 \in L_1$. Nous avons finalement que $\sum_{P \in L_1} I(P, L_1, C_0) \geq 4$ et, par conséquent, par le corollaire 45, $C_0 = FL_1$ où F est une conique.

(2) Notons M_{2k} un élément quelconque de la deuxième ligne de la matrice M.
1° Par le lemme 38,

$$\begin{aligned} I(M_{2k}, L_2, C_0) &\geq \min\{I(M_{2k}, L_2, C), I(M_{2k}, L_2, L), I(M_{2k}, L_2, \widetilde{L})\} \\ &\geq 1. \end{aligned}$$

De plus, par le lemme 37,

$$I(M_{2k}, L_2, C_0) = I(M_{2k}, L_2, F) + I(M_{2k}, L_2, L_1) \geq 1.$$

Si $M_{2k} \notin L_1$, alors $I(M_{2k}, L_2, L_1) = 0$ et donc $I(M_{2k}, L_2, F) \geq 1$.
2° Sinon, si $M_{2k} \in L_1$, alors $\exists j$ tel que $M_{2k} = M_{1j}$ et donc $M_{2k} \in$

$\widetilde{L}_j$. Par l'hypothèse de travail (i), $L_2 \cap \widetilde{L}_j = M_{2j}$ et par conséquent $j = k$. M_{2k} apparaît donc deux fois dans $\widetilde{L}_j$ car $M_{2k} = M_{1j} = M_{1k}$. Nous avons alors, par le lemme 38,

$$\begin{aligned} I(M_{2k}, \widetilde{L}_j, C_0) &\geq \min\{I(M_{2k}, \widetilde{L}_j, C), I(M_{2k}, \widetilde{L}_j, L), I(M_{2k}, \widetilde{L}_j, \widetilde{L})\} \\ &\geq 2. \end{aligned}$$

Par l'hypothèse de travail (i), $I(M_{2k}, \widetilde{L}_j, L_1) = 1$. Par le lemme 37,

$$I(M_{2k}, \widetilde{L}_j, C_0) = I(M_{2k}, \widetilde{L}_j, F) + I(M_{2k}, \widetilde{L}_j, L_1) \geq 2.$$

Nous avons finalement $I(M_{2k}, \widetilde{L}_j, F) \geq 1$; M_{2k} est donc un point de F et $I(M_{2k}, L_2, F) \geq 1$.
3° Comme $I(M_{2k}, L_2, F) \geq 1$ indépendamment du fait que $M_{2k} \in L_1$ ou non, nous avons $\sum_{P \in L_2} I(P, L_2, F) \geq 3$ et, par conséquent, par le corollaire 45, $F = DL_2$ où D est une droite.

(3) 1° Considérons le cas où $P_1 * Q_1 = P_2 * Q_2$. Appelons ce point commun $M_{3\cdot}$. Alors, par l'hypothèse de travail (i), $I(M_{3\cdot}, L_3, L_1) = I(M_{3\cdot}, L_3, L_2) = 0$. En effet, si $P_1 * Q_1 = P_2 * Q_2 = P_1 * P_2$ (les autres cas sont triviaux ou symétriques), alors $Q_1 * Q_2 = P_1 * P_2$ et les droites L_3 et $\widetilde{L}_3$ ont alors deux points communs. Par le lemme 38,

$$\begin{aligned} I(M_{3\cdot}, L_3, C_0) &\geq \min\{I(M_{3\cdot}, L_3, C), I(M_{3\cdot}, L_3, L), I(M_{3\cdot}, L_3, \widetilde{L})\} \\ &\geq 2. \end{aligned}$$

Or, par le lemme 37,

$$\begin{aligned} I(M_{3\cdot}, L_3, C_0) &= I(M_{3\cdot}, L_3, D) + I(M_{3\cdot}, L_3, L_2) + I(M_{3\cdot}, L_3, L_1) \\ &\geq 2, \end{aligned}$$

et donc $I(M_{3\cdot}, L_3, D) \geq 2$. Ce qui signifie, par la corollaire 45, que $D = kL_3$ où k est une constante non nulle.
2° Supposons que le point $M_{31} = P_1 * Q_1$ apparaisse n fois dans $\widetilde{L}_j$. Alors, par le lemme 38,

$$\begin{aligned} I(M_{31}, \widetilde{L}_j, C_0) &\geq \min\{I(M_{31}, \widetilde{L}_j, C), I(M_{31}, \widetilde{L}_j, L), I(M_{31}, \widetilde{L}_j, \widetilde{L})\} \\ &\geq n. \end{aligned}$$

De plus, par le lemme 37,

$$I(M_{31}, \widetilde{L}_j, C_0) = I(M_{31}, \widetilde{L}_j, D) + I(M_{31}, \widetilde{L}_j, L_1 L_2).$$

Or, par le lemme 37 et compte tenu de l'hypothèse de travail (i),

$$I(M_{31}, \widetilde{L}_j, L_1 L_2) = n - 1,$$

et donc $I(M_{31}, \widetilde{L}_j, D) \geq 1$. Cela signifie que $M_{31} \in D$. Comme le même argument est valable pour le point $M_{32} = P_2 * Q_2$, nous avons que $M_{32} \in D$. La droite D a par conséquent deux points distincts communs avec L_3 et donc, $D = kL_3$ où k est une constante non nulle.

Finalement, nous avons $C = kL_1L_2L_3 = kL$ où k est une constante non nulle. Or, par hypothèse, $C(R_2) = 0$ et $L(R_2) \neq 0$, ce qui est impossible car $k \neq 0$. Nous avons donc

$$a_1 C + a_2 L + a_3 \widetilde{L} = 0.$$

b) Montrons que $a_1 \neq 0$.
Par l'absurde, supposons que $a_1 = 0$, alors $a_2 \neq 0$ ou $a_3 \neq 0$. Par symétrie, supposons que $a_2 \neq 0$, alors L divise $\widetilde{L}$, et donc $\exists i, j$ tels que L_i est la même droite que $\widetilde{L}_j$, ce qui est contraire à l'hypothèse de travail (i). Nous avons démontré que

$$C = b_1 L + b_2 \widetilde{L}, \tag{IV.18}$$

avec $b_1 = a_2/a_1$ et $b_2 = a_3/a_1$.

c) Notons T le point d'intersection entre L_3 et $\widetilde{L}_3$. Par (IV.18), $C(T) = 0$; T est donc un point de C. Comme $T \in L_3 \cap C$, T est égal à

$$P_1 * Q_1, P_2 * Q_2 \text{ ou } (P_1 * Q_1) * (P_2 * Q_2). \tag{IV.19}$$

Et comme $T \in \widetilde{L}_3 \cap C$, T est égal à

$$P_1 * P_2, Q_1 * Q_2 \text{ ou } (P_1 * P_2) * (Q_1 * Q_2). \tag{IV.20}$$

Par l'hypothèse de travail (i), les deux premiers points de (IV.19) sont différents des deux premiers de (IV.20). En effet, si, par exemple, $P_1 * Q_1 = T = P_1 * P_2$, alors les droites L_1 et $\widetilde{L}_1$ ont deux points communs. Il reste donc les cas

$$(P_1 * Q_1) * (P_2 * Q_2) = T = (P_1 * P_2) * (Q_1 * Q_2), \tag{IV.21}$$

$$\begin{aligned} P_1 * Q_1 &= T = (P_1 * P_2) * (Q_1 * Q_2), \\ P_1 * P_2 &= T = (P_1 * Q_1) * (P_2 * Q_2), \\ P_2 * Q_2 &= T = (P_1 * P_2) * (Q_1 * Q_2), \\ Q_1 * Q_2 &= T = (P_1 * Q_1) * (P_2 * Q_2). \end{aligned} \tag{IV.22}$$

Si la relation (IV.21) est vérifiée, alors la démonstration est terminée. Les quatre dernières relations étant symétriques, nous allons uniquement montrer que la relation (IV.22) n'est jamais vérifiée ou implique la relation (IV.21). Considérons le point $M_{33} = (P_1 * Q_1) * (P_2 * Q_2)$. Ce point appartient à $C \cap L_3$. Donc, comme $c_2 \neq 0$ (car sinon C serait réductible), $M_{33} \in \widetilde{L}$, c.-à-d. M_{33} est un point de $\widetilde{L}_1, \widetilde{L}_2$ et/ou $\widetilde{L}_3$.
1° Si $M_{33} \in \widetilde{L}_1$, alors $M_{33} \in L_3 \cap \widetilde{L}_1$ et est donc égal à $P_1 * Q_1$, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = P_1 * Q_1.$$

Ce qui, remis dans (IV.22), termine la démonstration.
2° Si $M_{33} \in \widetilde{L}_2$, alors $M_{33} \in L_3 \cap \widetilde{L}_2$ et est donc égal à $P_2 * Q_2$, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = P_2 * Q_2. \qquad \text{(IV.23)}$$

Si $P_2 * Q_2 = P_1 * Q_1$, alors nous avons un cas équivalent à 1°. Sinon, par (IV.18) et par le lemme 38,

$$I(P_1 * Q_1, L_3, C) \geq \min\{I(P_1 * Q_1, L_3, L), I(P_1 * Q_1, L_3, \widetilde{L})\} \geq 2,$$

car, par (IV.22), $I(P_1 * Q_1, L_3, \widetilde{L}) \geq 2$. De plus, comme $P_1 * Q_1 \neq P_2 * Q_2$, par (IV.23),

$$I(P_2 * Q_2, L_3, C) = 2.$$

Nous avons finalement $\sum_{P \in L_3} I(P, L_3, C) \geq 4$; ce qui signifie, par le corollaire 45, que L_3 divise C, ce qui est impossible car C est irréductible.
3° Si $M_{33} \in \widetilde{L}_3$, alors $M_{33} \in L_3 \cap \widetilde{L}_3$ et est donc égal à T, i.e.

$$(P_1 * Q_1) * (P_2 * Q_2) = T = (P_1 * P_2) * (Q_1 * Q_2),$$

ce qui termine la démonstration.

(ii) Considérons à présent le cas où $\exists i, j$ tels que $L_i = \widetilde{L}_j$. Par symétrie, les seuls cas à envisager sont

$$\begin{aligned} P_1 &= Q_2, \\ P_1 &= Q_1 * Q_2 \quad (\text{et donc } P_1 * Q_1 = Q_2), \\ P_1 * P_2 &= P_1 * Q_1 \quad (\text{et donc } P_2 = Q_1). \end{aligned}$$

La relation (IV.16) devient alors respectivement

$$\begin{aligned} (P_1 * P_2) * (Q_1 * P_1) &= (P_1 * Q_1) * (P_2 * P_1), \\ (P_1 * P_2) * P_1 &= Q_2 * (P_2 * Q_2), \\ (P_1 * P_2) * (P_2 * Q_2) &= (P_1 * P_2) * (P_2 * Q_2). \end{aligned}$$

Comme la deuxième relation se réduit à $P_2 = P_2$ et que les deux autres relations sont immédiates, le théorème est démontré. □

Théorème 57. *Soit un corps infini K. Si $(E, \mathcal{O})$ est une courbe elliptique définie sur K, alors l'opération*

$$P + Q = \mathcal{O} * (P * Q) \tag{IV.24}$$

définit une structure de groupe commutatif ayant $\mathcal{O}$ comme élément neutre. De plus, si $\mathcal{O}'$ est un autre point de la courbe elliptique, alors l'opération

$$P +' Q = \mathcal{O}' * (P * Q)$$

définit une structure de groupe isomorphe au premier.

Preuve. (i) a) Vu la définition de la loi de composition de la sécante-tangente, la commutativité est évidente : $P + Q = \mathcal{O} * (P * Q) = \mathcal{O} * (Q * P) = Q + P$. b) $\mathcal{O}$ est l'élément neutre, car $P + \mathcal{O} = \mathcal{O} * (P * \mathcal{O}) = \mathcal{O} * (\mathcal{O} * P) = \mathcal{O} + P = P$. c) L'élément symétrique d'un élément Q est défini par :

$$-Q = (\mathcal{O} * \mathcal{O}) * Q. \tag{IV.25}$$

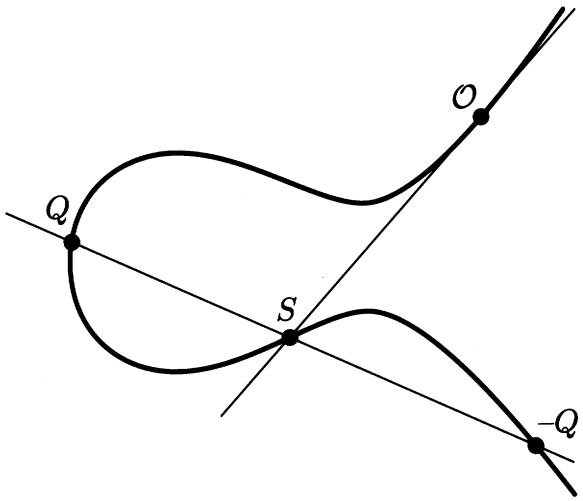


Figure 4: Symétrique d'un élément Q.

Ce qui est bien le symétrique, car

$$Q + (-Q) = \mathcal{O} * (Q * ((\mathcal{O} * \mathcal{O}) * Q)) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}$$

et

$$-Q + Q = \mathcal{O} * (((\mathcal{O} * \mathcal{O}) * Q) * Q) = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} + \mathcal{O} = \mathcal{O}.$$

d) Il reste à montrer l'associativité. Calculons :

$$\begin{aligned} P*(Q+R) &= P*(\mathcal{O}*(Q*R)) \\ &= ((P*Q)*Q)*(\mathcal{O}*(Q*R)) \quad \text{car } P=(P*Q)*Q \\ &= ((P*Q)*\mathcal{O})*(Q*(Q*R)) \quad \text{par la relation (IV.16)} \\ &= ((P*Q)*\mathcal{O})*R \quad \text{car } Q*(Q*R)=R \\ &= (\mathcal{O}*(P*Q))*R \\ &= (P+Q)*R. \end{aligned}$$

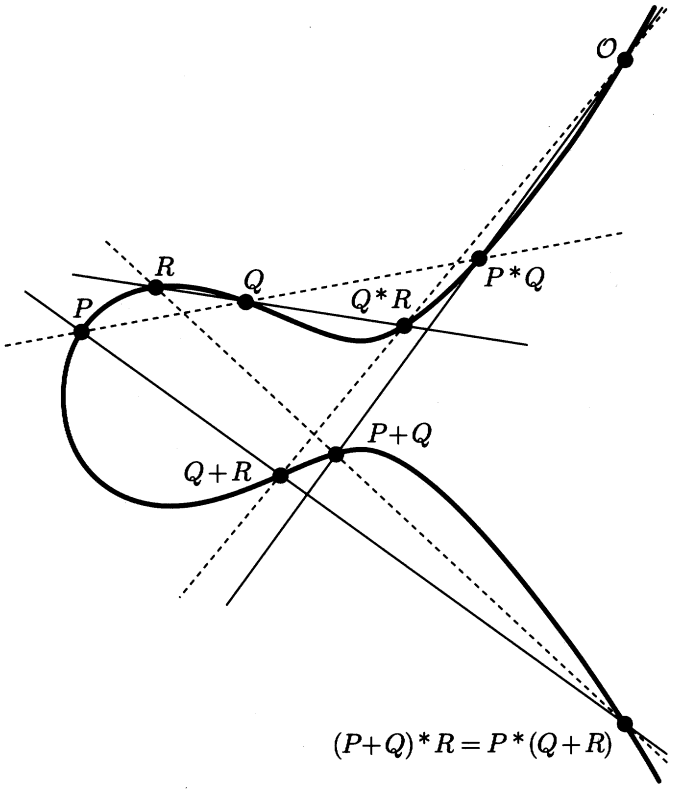


Figure 5: Vérification de l'associativité.

En appliquant $\mathcal{O}$ sur les deux membres de l'égalité, nous trouvons $P + (Q + R) = (P + Q) + R$.
(ii) Construisons l'application bijective

$$\phi : (E, +) \to (E, +'), P \mapsto P - \mathcal{O}',$$

alors

$$\phi(P + Q) = (P + Q) - \mathcal{O}'$$

$$
\begin{aligned}
&= \mathcal{O} * [(\mathcal{O} * (P * Q)) * ((\mathcal{O} * \mathcal{O}) * \mathcal{O}')] \\
&= \mathcal{O} * [(\mathcal{O} * (\mathcal{O} * \mathcal{O})) * ((P * Q) * \mathcal{O}')] \quad \text{par (IV.16)} \\
&= \mathcal{O} * [\mathcal{O} * (P +' Q)] \\
&= P +' Q = \phi(P) +' \phi(Q).
\end{aligned}
$$

L'application ϕ est donc un isomorphisme. □

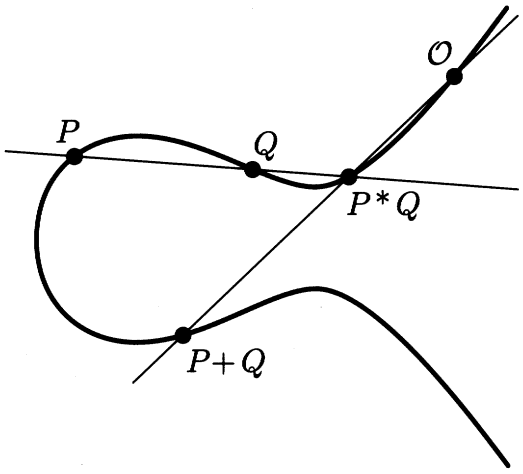


Figure 6: Loi de groupe sur une courbe elliptique.

IV.4.2 Théorème de Poincaré

Le théorème 57 peut être généralisé à un corps de caractéristique quelconque.

Théorème 58 Théorème de Poincaré. *Soit un corps K. Si $(E, \mathcal{O})$ est une courbe elliptique définie sur K, alors l'opération*

$$P + Q = \mathcal{O} * (P * Q)$$

définit une structure de groupe commutatif ayant $\mathcal{O}$ comme élément neutre. De plus, si $\mathcal{O}'$ est un autre point de la courbe elliptique, alors l'opération

$$P +' Q = \mathcal{O}' * (P * Q)$$

définit une structure de groupe isomorphe au premier.

Nous allons démontrer ce théorème dans le cas où $K = \mathbb{F}_q$. Pour cela, nous avons besoin d'introduire l'application *réduction modulo q*.

IV.4.3 L'application "réduction modulo q"

Notons $\mathbb{P}_2(\mathbb{Q})$, l'ensemble des points rationnels dans $\mathbb{P}_2$. Un point $P = (a, b, c)$ est *normalisé* si a, b et c sont des entiers sans facteur commun.

Exemple 16. Le point $(1/2, -2/3, 3/4)$ est représenté par $(6, -8, 9)$ en coordonnées normalisées.

Si $\widetilde{x}$ représente le résidu de x modulo q, i.e. $\widetilde{x} = x \bmod q$, alors à chaque point normalisé $P = (a, b, c)$ de $\mathbb{P}_2(\mathbb{Q})$ correspond, au signe près, un et un seul point $\widetilde{P} = (\widetilde{a}, \widetilde{b}, \widetilde{c})$ de $\mathbb{P}_2(\mathbb{F}_q)$, car au moins un des trois nombres a, b ou c n'est pas un multiple de q.

Définition 59. L'application *réduction modulo* q est l'application

$$\varphi : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{F}_q), P \mapsto \widetilde{P}. \tag{IV.26}$$

Soit $C \in \mathbb{Q}[X, Y, Z]_d$ une courbe définie sur $\mathbb{Q}$ dont les coefficients sont normalisés, nous dirons que C est *normalisée*. Alors, nous associons la courbe $\widetilde{C} \in \mathbb{F}_q[X, Y, Z]_d$ en réduisant les coefficients de C modulo q.

Proposition 60. *Avec les notations précédentes, si* $P \in C(\mathbb{Q})$, *alors* $\widetilde{P} \in \widetilde{C}(\mathbb{F}_q)$.

Preuve. Comme $\psi : \mathbb{Z} \to \mathbb{F}_q, x \mapsto \widetilde{x}$ est un homomorphisme de groupe, la thèse est immédiate. □

Corollaire 61. *Si* C_1 *et* C_2 *sont deux courbes, alors*

$$\widetilde{(C_1(\mathbb{Q}) \cap C_2(\mathbb{Q}))} \subseteq \widetilde{C_1}(\mathbb{F}_q) \cap \widetilde{C_2}(\mathbb{F}_q).$$

Preuve. Trivial. □

Lemme 62. *Soit une droite normalisée* $L \in \mathbb{P}_2(\mathbb{Q})$ *donnée par*

$$L : aX + bY + cZ = 0.$$

Alors il existe une tranformation linéaire

$$T : \mathbb{P}_2(\mathbb{Q}) \to \mathbb{P}_2(\mathbb{Q}), \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$$

compatible avec la réduction modulo q *qui transforme* L *en la droite à l'infini* $L' : Z' = 0$.

Preuve. Notons $d = \text{pgcd}(b, c)$. Par le corollaire 4, $\exists r, s \in \mathbb{Z}$ tels que $rc - sb = d$. Remarquons que r et s sont nécessairement premiers entre eux. De plus, comme L est en coordonnées normalisées, $\text{pgcd}(a, d) = 1$, et donc, par le corollaire 5, $\exists t, u \in \mathbb{Z}$ tels que $td + ua = 1$. Comme $\text{pgcd}(r, s) = 1$, $\exists v, w \in \mathbb{Z} : vs - wr = u$. Définissons la matrice (t_{ij}) :

$$(t_{ij}) = \begin{pmatrix} t & v & w \\ 0 & r & s \\ a & b & c \end{pmatrix}.$$

Le déterminant de cette matrice vaut 1 par les hypothèses sur r, s, t, u, v et w. Par conséquent, la matrice $(m_{ij}) = (t_{ij})^{-1}$ aura des éléments entiers. Les matrices réduites $(\widetilde{t}_{ij})$ et $(\widetilde{m}_{ij})$ sont donc inverses l'une de l'autre, fournissant un changement de coordonnées correspondant modulo q. □

Proposition 63. *Soient une cubique irréductible non singulière C et une droite L définies sur $\mathbb{Q}$. Alors, si $C \cap L = \{P_1, P_2, P_3\}$ en coordonnées normalisées et si $\widetilde{L}$ n'est pas une composante de $\widetilde{C}$, $\widetilde{C} \cap \widetilde{L} = \{\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}\}$.*

Preuve. (i) Supposons que L soit la droite à l'infini $Z = 0$. Notons $P_i = (a_i, b_i, 0)$ $(i = 1, 2, 3)$, les trois points d'intersection de C et de L en coordonnés normalisées et $F(X, Y, Z) = 0$, l'équation de C. Alors,

$$F(X, Y, 0) = k \prod_{i=1}^{3} (a_i Y - b_i X), \tag{IV.27}$$

avec $k \neq 0$ car C est irréductible. Comme $\widetilde{L}$ n'est pas une composante de $\widetilde{C}$, il s'ensuit que $\widetilde{F}(X, Y, 0) \neq 0 \ \forall X, Y$. Par ailleurs, étant donné que les points P_i sont en coordonnées normalisées, $(\widetilde{a}_i, \widetilde{b}_i) \neq (0, 0)$; et donc $\widetilde{k} \neq 0$. Nous pouvons par conséquent réduire (IV.27) modulo q :

$$\widetilde{F}(X, Y, 0) = \widetilde{k} \prod_{i=1}^{3} (\widetilde{a}_i Y - \widetilde{b}_i X),$$

et donc, $\widetilde{C} \cap \widetilde{L} = \{\widetilde{P_1}, \widetilde{P_2}, \widetilde{P_3}\}$.
(ii) Si L n'est pas la droite à l'infini, alors nous l'y ramenons par la transformation définie par le lemme 62. □

IV.4.4 Démonstration du théorème de Poincaré

Par le théorème 57, nous savons que si $(E, \mathcal{O})$ est une courbe elliptique définie sur $\mathbb{Q}$, alors l'opération $P + Q = \mathcal{O} * (P * Q)$ définit une structure de groupe.

Nous devons donc démontrer que, si $(\widetilde{E}, \widetilde{\mathcal{O}})$ est une courbe elliptique définie sur $\mathbb{F}_q$, l'application modulo $q : E(\mathbb{Q}) \to \widetilde{E}(\mathbb{F}_q), P \mapsto \widetilde{P}$ est un homomorphisme de groupe.

Preuve. Soient P et Q deux points de $E(\mathbb{Q})$ tels que $P + Q = R$. Notons respectivement L_1 et L_2, les droites PQ et $(P * Q)R$; et donc

$$E \cap L_1 = \{P, Q, P * Q\} \quad \text{et} \quad E \cap L_2 = \{P * Q, R, \mathcal{O}\}.$$

Par la proposition 63,

$$\widetilde{E} \cap \widetilde{L_1} = \{\widetilde{P}, \widetilde{Q}, \widetilde{P * Q}\} \quad \text{et} \quad \widetilde{E} \cap \widetilde{L_2} = \{\widetilde{P * Q}, \widetilde{R}, \widetilde{\mathcal{O}}\},$$

et donc $\widetilde{R} = \widetilde{P + Q} = \widetilde{P} + \widetilde{Q}$. □

Il reste à montrer que cette structure de groupe est indépendante du choix de $\widetilde{\mathcal{O}} \in \widetilde{E}(\mathbb{F}_q)$.

Preuve. Construisons l'application bijective

$$\phi : (\widetilde{E}, +) \to (\widetilde{E}, +'), \widetilde{P} \mapsto \widetilde{P} - \widetilde{\mathcal{O}'},$$

alors, par le théorème 57 et comme l'application modulo q est un homomorphisme de $E(\mathbb{Q})$ dans $\widetilde{E}(\mathbb{F}_q)$,

$$\begin{aligned}\phi(\widetilde{P} + \widetilde{Q}) = \phi(\widetilde{P + Q}) &= (\widetilde{P + Q}) - \widetilde{\mathcal{O}'} = (\widetilde{P} + \widetilde{Q}) - \widetilde{\mathcal{O}'} = \widetilde{P} +' \widetilde{Q} \\ &= \phi(\widetilde{P}) +' \phi(\widetilde{Q}).\end{aligned}$$

L'application ϕ est donc un isomorphisme. □

IV.4.5 Formules explicites

Nous allons à présent donner les formules explicites pour additionner deux points P et Q et pour doubler un point P sur une courbe elliptique donnée par l'équation de Weierstrass

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0 \qquad \text{(IV.28)}$$

où nous prenons, comme élément neutre, le point à l'infini $\mathcal{O} = (0, 1, 0)$. Étant donné que $\mathcal{O}$ est le seul point à l'infini, nous allons travailler en coordonnées non homogènes.

Soient $P = (p_1, p_2)$ et $Q = (q_1, q_2)$ deux points distincts de E.

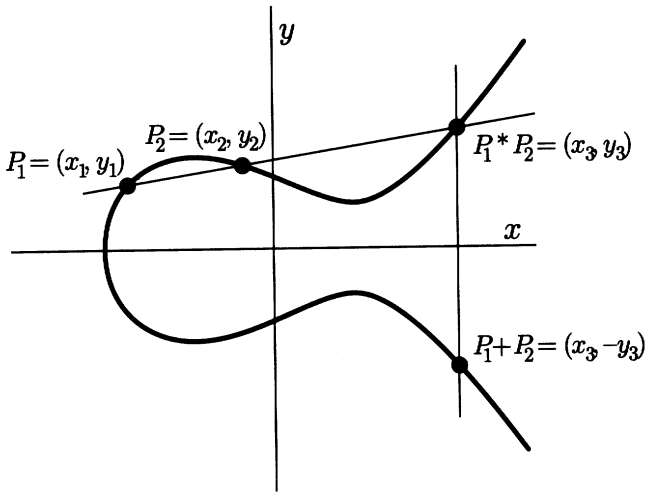


Figure 7: Addition de deux points sur une courbe de Weierstrass.

Calculons $-P = (x_{(-P)}, y_{(-P)})$, l'inverse du point P. Ce point appartient à la droite $L : x = p_1$, car $\mathcal{O} * \mathcal{O} = \mathcal{O}$. En substituant dans (IV.28), nous obtenons

$$\begin{aligned} f(p_1, y) &= y^2 + a_1 p_1 y + a_3 y - p_1^3 - a_2 p_1^2 - a_4 p_1 - a_6 \\ &= c(y - p_2)(y - y_{(-P)}) \\ &= cy^2 - c(p_2 + y_{(-P)})y + c p_2 y_{(-P)}. \end{aligned}$$

Si nous égalons les coefficients, nous avons $c = 1$ et $a_1 p_1 + a_3 = c(p_2 + y_{(-P)})$, et donc

$$-P = (p_1, -p_2 - a_1 p_1 - a_3). \tag{IV.29}$$

Addition des points P et Q (i) Si $p_1 = q_1$ et si $q_2 = -p_2 - a_1 p_1 - a_3$, alors

$$P + Q = \mathcal{O}.$$

(ii) Notons $R = (r_1, r_2)$, la somme de P et de Q. Remarquons que R n'est pas le point à l'infini (cas (i)). Supposons que $q_2 \neq -p_2 - a_1 p_1 - a_3$.
a) Si $p_1 \neq q_1$, posons

$$\lambda = \frac{q_2 - p_2}{q_1 - p_1} \quad \text{et} \quad \gamma = p_2 - \lambda p_1.$$

La sécante passant par P et Q a pour équation $y = \lambda x + \gamma$. En substituant dans (IV.28), nous avons

$$\begin{aligned} f(x\ ,\ \lambda x+\gamma) &= (\lambda x+\gamma)^2 + a_1 x(\lambda x+\gamma) + a_3(\lambda x+\gamma) - x^3 - a_2 x^2 - a_4 x - a_6 \\ &= -x^3 + (-a_2 + \lambda^2 + a_1\lambda)x^2 + (-a_4 + 2\lambda\gamma + a_1\gamma + a_3\lambda)x \\ &\qquad -a_6 + \gamma^2 + a_3\gamma \\ &= c(x-p_1)(x-q_1)(x-r_1) \\ &= cx^3 - c(p_1+q_1+r_1)x^2 + c(q_1r_1+p_1q_1+p_1r_1)x - cp_1q_1r_1. \end{aligned}$$

Si nous égalons les coefficients, nous avons $c=-1$ et $-c(p_1+q_1+r_1) = -a_2+\lambda^2+a_1\lambda$, et donc

$$r_1 = -a_2 + \lambda^2 + a_1\lambda - p_1 - q_1, \tag{IV.30}$$
$$r_2 = -(\lambda r_1 + \gamma) - a_1 r_1 - a_3. \tag{IV.31}$$

b) Si $p_1 = q_1$, alors $P = Q$. L'addition de P et de Q revient alors à doubler le point P.

Doublement du point P Les formules vues ci-dessus restent valables, si ce n'est que maintenant λ représente le coefficient angulaire de la tangente à la courbe en P :

$$\lambda = \left.\frac{dy}{dx}\right|_P = -\frac{\frac{\partial f}{\partial x}(p_1,p_2)}{\frac{\partial f}{\partial y}(p_1,p_2)} = \frac{3p_1^2 + 2a_2p_1 + a_4 - a_1p_2}{2p_2 + a_1p_1 + a_3}.$$

Exemple 17. Soit la courbe elliptique

$$y^2 = x^3 + x + 1$$

définie sur $\mathbb{F}_{23}$. Les seuls points de cette courbe sont

$$\begin{array}{cccccccccc} (0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) & (5,4) & (5,19) \\ (6,4) & (6,19) & (7,11) & (7,12) & (9,7) & (9,16) & (11,3) & (11,20) & (12,4) \\ (12,19) & (13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & (19,5) & (19,18) \end{array}$$

plus le point à l'infini $\mathcal{O}$. Prenons $P=(3,10)$ et $Q=(9,7)$. Calculons $R = P+Q$. Les formules précédentes donnent

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} = 11 \in \mathbb{F}_{23} \quad \text{et} \quad \gamma = 10 - 11\cdot 3 = -23 = 0 \in \mathbb{F}_{23},$$

$$\begin{cases} r_1 = -0 + 11^2 + 0\cdot 11 - 3 - 9 = 109 = 17 \in \mathbb{F}_{23} \\ r_2 = -(11\cdot 17 + 0) - 0\cdot 17 - 0 = -187 = -3 = 20 \in \mathbb{F}_{23} \end{cases}.$$

Par conséquent, $(3,10)+(9,7)=(17,20)$. Calculons maintenant $R=2P$. Les formules précédentes donnent

$$\lambda=\frac{3\cdot 3^2+2\cdot 0\cdot 3+1-0\cdot 10}{2\cdot 10+0\cdot 3+0}=\frac{28}{20}=\frac{5}{20}=\frac{1}{4}=6,$$

$$\gamma=10-6\cdot 3=-8=15,$$

$$\begin{cases} r_1=-0+6^2+0\cdot 6-3-3=30=7 \\ r_2=-(7\cdot 6+15)-0\cdot 6-0=-57=-11=12. \end{cases}.$$

Par conséquent, $2(3,10)=(7,12)$.

Exemple 18. Soient le corps $\mathbb{F}_{2^4}$ généré par la racine α du polynôme irréductible sur $\mathbb{F}_2$ donné par $f(x)=x^4+x+1$ et la courbe elliptique

$$y^2+xy=x^3+\alpha^4x^2+1$$

définie sur $\mathbb{F}_{2^4}$. Avant toute chose, calculons les puissances successives de α

$$\begin{aligned}
\alpha^0&=[0001],\\
\alpha^1&=[0010],\\
\alpha^2&=[0100],\\
\alpha^3&=[1000],\\
\alpha^4&=\alpha+1=[0011],\\
\alpha^5&=\alpha^2+\alpha=[0110],\\
\alpha^6&=\alpha^3+\alpha^2=[1100],\\
\alpha^7&=\alpha^4+\alpha^3=\alpha^3+\alpha+1=[1011],\\
\alpha^8&=\alpha^4+\alpha^2+\alpha=\alpha^2+1=[0101],\\
\alpha^9&=\alpha^3+\alpha=[1010],\\
\alpha^{10}&=\alpha^4+\alpha^2=\alpha^2+\alpha+1=[0111],\\
\alpha^{11}&=\alpha^3+\alpha^2+\alpha=[1110],\\
\alpha^{12}&=\alpha^4+\alpha^3+\alpha^2=\alpha^3+\alpha^2+\alpha+1=[1111],\\
\alpha^{13}&=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+1=[1101],\\
\alpha^{14}&=\alpha^4+\alpha^3+\alpha=\alpha^3+1=[1001],\\
\alpha^{15}&=\alpha^4+\alpha=1=[0001].
\end{aligned}$$

Remarquons que pour être cohérent avec nos notations, nous aurions dû écrire l'équation de la courbe sous la forme

$$[0001]y^2+[0001]xy=[0001]x^3+[0011]x^2+[0001],$$

mais comme [0001] est l'identité multiplicative, la première écriture est correcte. Les seuls points de cette courbe sont

$$\begin{array}{cccccccc} (0,1) & (1,\alpha^6) & (1,\alpha^{13}) & (\alpha^3,\alpha^8) & (\alpha^3,\alpha^{13}) & (\alpha^5,\alpha^3) & (\alpha^5,\alpha^{11}) & (\alpha^6,\alpha^8) \\ (\alpha^6,\alpha^{14}) & (\alpha^9,\alpha^{10}) & (\alpha^9,\alpha^{13}) & (\alpha^{10},\alpha^1) & (\alpha^{10},\alpha^8) & (\alpha^{12},0) & (\alpha^{12},\alpha^{12}) & \end{array}$$

plus le point à l'infini $\mathcal{O}$. Prenons $P = (\alpha^6, \alpha^8)$ et $Q = (\alpha^3, \alpha^{13})$. Calculons $R = P + Q$. Par les formules précédentes,

$$\lambda = \frac{\alpha^{13} - \alpha^8}{\alpha^3 - \alpha^6} = \frac{(\alpha^3 + \alpha^2 + 1) + (\alpha^2 + 1)}{(\alpha^3) + (\alpha^3 + \alpha^2)} = \frac{\alpha^3}{\alpha^2} = \alpha,$$

$$\gamma = \alpha^8 - \alpha\alpha^6 = \alpha^8 + \alpha^7 = (\alpha^2) + (\alpha^3 + \alpha + 1) = \alpha^3 + \alpha^2 + \alpha = \alpha^{11},$$

$$\begin{cases} r_1 = -\alpha^4 + \alpha^2 + 1 \cdot \alpha - \alpha^6 - \alpha^3 = (\alpha + 1) + \alpha^2 + \alpha + (\alpha^3 + \alpha^2) + \alpha^3 \\ \quad = 1 \\ r_2 = -(\alpha \cdot 1 + \alpha^{11}) - 1 \cdot 1 - 0 = \alpha^3 + \alpha^2 + 1 = \alpha^{13} \end{cases}.$$

Par conséquent, $(\alpha^6, \alpha^8) + (\alpha^3, \alpha^{13}) = (1, \alpha^{13})$ ou de façon équivalente,

$$([1100],[0101]) + ([1000],[1101]) = ([0001],[1101]).$$

Calculons maintenant $R = 2P$. Par les formules précédentes,

$$\lambda = \frac{3\alpha^{12} + 2\alpha^4\alpha^6 + 0 - 1 \cdot \alpha^8}{2\alpha^8 + 1 \cdot \alpha^6 + 0} = \frac{\alpha^{12} + \alpha^8}{\alpha^6} = +\alpha^6 + \alpha^2 = \alpha^3,$$

$$\gamma = \alpha^8 - \alpha^3\alpha^6 = (\alpha^2 + 1) + (\alpha^3 + \alpha) = \alpha^{12},$$

$$\begin{cases} r_1 = -\alpha^4 + \alpha^6 + 1 \cdot \alpha^3 - \alpha^6 - \alpha^6 = \alpha^4 + \alpha^6 + \alpha^3 = \alpha^2 + \alpha + 1 = \alpha^{10} \\ r_2 = -(\alpha^3\alpha^{10} + \alpha^{12}) - 1 \cdot \alpha^{10} - 0 = \alpha^{13} + \alpha^{12} + \alpha^{10} = \alpha^2 + 1 = \alpha^8 \end{cases}.$$

Par conséquent, $2(\alpha^6, \alpha^8) = (\alpha^{10}, \alpha^8)$ ou de façon équivalente,

$$2([1100],[0101]) = ([0111],[0101]).$$

À retenir.

▶ Soit un corps K. Une *courbe elliptique* est une cubique irréductible non singulière de $\mathbb{P}_2(K)$ qui possède un point $\mathcal{O}$.

▶ Une *courbe elliptique* est une courbe birationnellement équivalente aux points de l'équation de Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

plus le point à l'infini $\mathcal{O} = (0, 1, 0)$.

▶ Si $(E, \mathcal{O})$ est une courbe elliptique, alors l'opération $P+Q = \mathcal{O}*(P*Q)$ définit à un isomorphisme près une structure de *groupe commutatif* dont $\mathcal{O}$ est l'élément neutre où la loi de composition $P * Q$ définit le troisième point d'intersection de la droite passant passant par P et Q avec la courbe elliptique.

▶ Si une courbe elliptique est donnée par une équation de Weierstrass plus le point à l'infini $\mathcal{O}$, alors l'addition de deux points $P = (p_1, p_2)$ et $Q = (q_1, q_2)$ vaut

$\mathcal{O}$ si $q_1 = p_1$ et si $q_2 = -p_2 - a_1p_1 - a_3$;

$R = (r_1, r_2)$ où

$$\begin{cases} r_1 = -a_2 + \lambda^2 + a_1\lambda - p_1 - q_1, \\ r_2 = -(\lambda r_1 + \gamma) - a_1r_1 - a_3; \end{cases}$$

avec

$$\lambda = \frac{q_2 - p_2}{q_1 - p_1} \quad \text{si} \quad p_1 \neq q_1,$$
$$\lambda = \frac{3p_1^2 + 2a_2p_1 + a_4 - a_1p_2}{2p_2 + a_1p_1 + a_3} \quad \text{si} \quad p_1 = q_1$$
$$\text{et} \quad \gamma = p_2 - \lambda p_1.$$

Remarquons que $y = \lambda x + \gamma$ est soit la sécante passant par P et Q, soit la tangente à la courbe si $P = Q$.

Partie V
Applications

Résumé. Le domaine d'applications des courbes elliptiques est très vaste. Dans cette partie, nous allons uniquement voir comment d'une part, il est possible de prouver la primalité d'un nombre et d'autre part, comment il est possible de factoriser un nombre composé à l'aide des courbes elliptiques. Finalement, nous allons voir que les courbes elliptiques sont également utiles en cryptographie.

V.1 Test de primalité et factorisation

V.1.1 Introduction

Les problèmes de primalité et de factorisation sont intimement liés, c'est pourquoi nous allons les traiter simultanément.

Proposition 64 (Petit théorème de Fermat). *Soit un nombre premier p. Tout entier a satisfait à $a^p \equiv a \pmod{p}$. De plus, si a n'est pas divisible par p, alors $a^{p-1} \equiv 1 \pmod{p}$.*

Preuve. (i) Considérons d'abord le cas où $p \nmid a$, alors $a \in \mathbb{F}_p^*$. Par conséquent, par le théorème 7 où nous prenons $G = \mathbb{F}_p^*$, nous avons $a^{p-1} \equiv 1 \pmod{p}$. Si nous multiplions les deux membres par a, nous obtenons la thèse.
(ii) Si $p \mid a$, alors $a \equiv 0 \pmod{p}$ et la thèse est triviale. □

Le petit théorème de Fermat permet d'introduire la notion de nombres pseudo-premiers.

Définition 65. Un nombre *pseudo-premier en base b* est un nombre composé impair n qui ne divise pas b et tel que

$$b^{n-1} \equiv 1 \pmod{n}. \tag{V.1}$$

Notation. Un nombre n pseudo-premier en base b sera noté "psp(b)".

Cependant, il existe des nombres n qui sont pseudo-premiers pour toute base b, ce sont les *nombres de Carmichael*.

Définition 66. Soit p un nombre premier impair qui ne divise pas a. S'il existe un entier x tel que $a \equiv x^2 \pmod{p}$, alors a est appelé *résidu quadratique modulo* p ; sinon a est appelé un *non-résidu quadratique modulo* p.

Notation. Legendre a introduit la notation suivante :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p \text{ divise } a, \\ +1 \text{ si } a \text{ est un résidu quadratique modulo } p, \\ -1 \text{ sinon.} \end{cases}$$

Par la suite, Jacobi a étendu le symbole de Legendre à un nombre impair $n = \prod_{i=1}^{t} p_i^{e_i}$:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{t} \left(\frac{a}{p_i}\right)^{e_i}.$$

Proposition 67 (Critère d'Euler). *Si p est un nombre premier impair qui ne divise pas b, alors*

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}.$$

Preuve. Soit g un générateur du groupe $\mathbb{F}_p^*$. Cherchons les valeurs de s pour lesquelles $g^s \equiv -1 \pmod{p}$. Si $g^s \equiv -1 \pmod{p}$, alors il faut que $g^{2s} \equiv 1 \pmod{p}$. Cette condition signifie que $2s$ doit être un multiple de $p-1$, i.e. $s = 0, (p-1)/2, p-1, \ldots$ Or, comme $g, g^2, \ldots, g^{p-1}$ modulo p constituent tous les éléments de $\mathbb{F}_p^*$ et que $g^{p-1} \equiv 1 \pmod{p}$, on obtient finalement $s = (p-1)/2$. Si on représente b par $b \equiv g^t \bmod p$, alors

$$b^{(p-1)/2} \equiv g^{t(p-1)/2} \equiv \begin{cases} g^{(p-1)k} \equiv 1 \pmod{p} & \text{si } t = 2k, \\ g^{(p-1)k} g^{(p-1)/2} \equiv -1 \pmod{p} & \text{si } t = 2k+1. \end{cases}$$

□

Ce critère d'Euler introduit une nouvelle sorte de nombres pseudo-premiers.

Définition 68. Un nombre *pseudo-premier d'Euler en base* b est un nombre composé impair n qui ne divise pas b et tel que

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}. \tag{V.2}$$

Notation. Un nombre n pseudo-premier d'Euler en base b sera noté "e-psp(b)".

Enfin, Miller et Rabin ont proposé un test de pseudo-primalité meilleur que ceux de Fermat ou d'Euler (voir proposition 70) et qui, de surcroît, "arrête" les nombres de Carmichael. Leur méthode repose sur la notion de nombres pseudo-premiers forts.

Définition 69. Un nombre *pseudo-premier fort en base* b est un nombre composé impair $n = 2^s t + 1$ (avec t impair et $s > 0$) qui ne divise pas b et tel que

$$b^t \equiv 1 \pmod{n} \text{ ou } \exists r, 0 \leq r < s \text{ t.q. } b^{2^r t} \equiv -1 \pmod{n}.$$

Notation. Un nombre n pseudo-premier fort en base b sera noté "spsp(b)".

Proposition 70. *Si N est spsp(b) ou epsp(b), alors N est psp(b).*

Preuve. (i) Soient $N = 2^s t + 1$ (avec $s > 0$ et t impair), un nombre pseudo-premier fort et b, une base telle que $\text{pgcd}(b, N) = 1$. Alors,

$$b^{N-1} - 1 \equiv b^{2^s t} - 1 \equiv (b^t - 1)(b^t + 1)(b^{2t} + 1) \cdots (b^{2^{s-1} t} + 1) \equiv 0 \pmod{N}.$$

(ii) Si N est epsp(b), alors $b^{N-1} \equiv \left(\frac{b}{N}\right)^2 \equiv 1 \pmod{N}$. □

Selfridge a démontré qu'un nombre *spsp*(b) est également *epsp*(b). Il y a par conséquent davantage de nombres pseudo-premiers (simples) et pseudo-premiers d'Euler que de nombres pseudo-premiers forts. C'est donc ces derniers qui seront considérés dans les tests de pseudo-primalité.

L'algorithme de Miller-Rabin consiste à vérifier qu'un candidat premier N est spsp(b) pour $b = 2, 3, 5, 7, 11, \ldots$ La probabilité que ce test échoue est inférieure à 4^{-s} où s est le nombre de bases pour lesquelles N est pseudo-premier fort. En pratique, nous effectuerons 10 tests de Miller-Rabin ; la probabilité que N est composé sera alors inférieure à $9,5 \cdot 10^{-7}$. Il existe de vrais tests de primalité, mais ceux-ci sont plus coûteux. Un test de pseudo-primalité sera donc effectué avant d'utiliser un tel test. Il est à noter que les tests de pseudo-primalité constituent également des tests de composition : si un nombre ne passe pas à travers un tel test, alors il est composé.

Dans la suite, nous noterons N le candidat premier ou le nombre dont nous cherchons la décomposition première et p un nombre premier.

Mais avant tout, nous allons démontrer le théorème de Hasse qui encadre la cardinalité d'un courbe elliptique définie sur $\mathbb{F}_q$. Nous allons uniquenment démontrer ce théorème dans le cas où $q = p$ est un nombre premier. Il faut toutefois retenir que ce théorème reste valable si q est une puissance d'un nombre premier p.

V.1.2 Théorème de Hasse

Théorème 71 (Théorème de Hasse). *Si E est une courbe elliptique définie sur $\mathbb{F}_p$, alors*

$$|p+1-\#E(\mathbb{F}_p)| \leq 2\sqrt{p}.$$

Preuve. Notons $m = \#E(\mathbb{F}_p)$.
(i) Si $p = 2$ ou $p = 3$, alors la thèse devient respectivement

$$1 \leq m \leq 5 \quad \text{et} \quad 1 \leq m \leq 7,$$

ce qui est trivialement respecté car $\mathcal{O} \in E(\mathbb{F}_p)$ et, que vu les relations (IV.5) à (IV.8), nous voyons qu'à chaque abscisse x correspond au plus deux ordonnées y.
(ii) Supposons que la courbe elliptique E soit donnée par l'équation de Weierstrass

$$E : y^2 = x^3 + ax + b \cup \mathcal{O} = (0,1,0).$$

1) Considérons la courbe elliptique

$$Y^2 = \frac{X^3 + aX + b}{x^3 + ax + b} \cup \mathcal{O} = (0,1,0) \tag{V.3}$$

avec X et $Y \in \mathbb{F}_p(x)$, le corps des fractions rationnelles à coefficients dans $\mathbb{F}_p$. Par le théorème 57, l'ensemble des solutions de (V.3) forme un groupe commutatif et comme $(x,1)$ et $(x^p, (x^3+ax+b)^{\frac{1}{2}(p-1)})$ sont solutions de (V.3), il s'ensuit que

$$Z_n = (x^p, (x^3+ax+b)^{\frac{1}{2}(p-1)}) + n(x,1) \tag{V.4}$$

vérifie également (V.3). Définissons d_n :

$$\begin{cases} d_n = 0 \quad \text{si } Z_n = \mathcal{O}, \\ d_n = \max(\deg(\text{numérateur}(X_n)), \deg(\text{dénominateur}(X_n)))^\dagger \\ \qquad\qquad\qquad\qquad \text{si } Z_n = (X_n, Y_n) \neq \mathcal{O}, \end{cases}$$

où X_n est écrit de façon telle que

$$\text{pgcd}(\text{numérateur}(X_n), \text{dénominateur}(X_n)) = 1.$$

D'abord, calculons l'analogue des formules (IV.29), (IV.30) et (IV.31) pour une courbe elliptique donnée sous la forme

$$E' : F(X,Y) = Y^2 - \frac{X^3 + aX + b}{x^3 + ax + b}. \tag{V.5}$$

†Si $f \in K[x]$, alors $\deg(f(x))$ désigne le degré du polynôme f.

Soient $P = (P_1, P_2)$ et $Q = (Q_1, Q_2)$ deux points distincts de E', tous deux différents de $\mathcal{O}$ et tels que $R = (R_1, R_2) = P + Q \neq \mathcal{O}$. L'inverse de point P est donné par

$$-P = (P_1, -P_2), \tag{V.6}$$

celui-ci s'obtient immédiatement par des arguments similiaires à ceux utilisés pour obtenir la formule (IV.29). Notons $\lambda X + \gamma$ la sécante passant par P et Q avec

$$\lambda = \frac{Q_2 - P_2}{Q_1 - P_1} \quad \text{et} \quad \gamma = P_2 - \lambda P_1.$$

En substituant dans (V.5), nous avons

$$\begin{aligned} F(X, \lambda X + \gamma) &= \frac{-X^3}{x^3 + ax + b} + \lambda^2 X^2 + \left[2\lambda\gamma - \frac{a}{x^3 + ax + b}\right] X \\ &\quad + \left[\gamma^2 - \frac{b}{x^3 + ax + b}\right] \\ &= c(X - P_1)(X - P_2)(X - P_3) \\ &= cX^3 - c(P_1 + Q_1 + R_1)X^2 \\ &\quad + c(Q_1R_1 + P_1Q_1 + P_1R_1)X - cP_1Q_1R_1. \end{aligned}$$

Par conséquent $c = -(x^3 + ax + b)^{-1}$ et $-c(P_1 + Q_1 + R_1) = \lambda^2$, et

$$R_1 = \lambda^2(x^3 + ax + b) - P_1 - Q_1, \tag{V.7}$$

$$R_2 = -(\lambda R_1 + \gamma). \tag{V.8}$$

Remarquons que si $P = Q$, alors la sécante devient tangente et

$$\lambda = -\frac{\frac{\partial F}{\partial X}(P_1, P_2)}{\frac{\partial F}{\partial Y}(P_1, P_2)} = \frac{3P_1^2 + a}{2P_2(x^3 + ax + b)}. \tag{V.9}$$

2) Montrons que $d_{-1} - d_0 = m - p$.
Par (V.4), nous avons immédiatement que

$$d_0 = p. \tag{V.10}$$

Il reste à montrer que $d_{-1} = m$. Par (V.6) et (V.7),

$$\begin{aligned} X_{-1} &= (x^p, (x^3 + ax + b)^{\frac{1}{2}(p-1)}) + (x, -1) \\ &= \underbrace{\left(\frac{-1 - (x^3 + ax + b)^{\frac{1}{2}(p-1)}}{x - x^p}\right)^2 (x^3 + ax + b)}_{L} - x^p - x. \end{aligned}$$

Simplifions la fraction L. Dans $(\mathbb{Z}/p\mathbb{Z})$, le dénominateur de L se factorise par la proposition 64 en

$$(x - x^p)^2 = \prod_{u \in (\mathbb{Z}/p\mathbb{Z})} (x - u)^2.$$

Les facteurs de la forme $(x - u)$ du numérateur de L sont ceux pour lesquels ce numérateur s'annulle en u. Cela apparaît quand

$$(u^3 + ax + b)^{\frac{p-1}{2}} = -1 \iff \left(\frac{u^3 + au + b}{p}\right) = -1$$

par la proposition 67, et quand

$$u^3 + ax + b = 0 \iff \left(\frac{u^3 + au + b}{p}\right) = 0.$$

Après simplification, les facteurs restants dans le dénominateur sont

$$(x - u)^2 \text{ si } \left(\frac{u^3 + au + b}{p}\right) = 1, \text{ et } (x - u) \text{ si } \left(\frac{u^3 + au + b}{p}\right) = 0,$$

ce qui correspond au nombre de solutions affines de $E(\mathbb{F}_p)$ et donc

$$\deg(\text{dénominateur}(L)) = m - 1.$$

Or,

$$X_{-1} = \frac{x^{2p+1} + R(x)}{(x - x^p)^2}$$

où le degré de $R(x)$ est strictement inférieur à $2p + 1$; donc

$$\deg(\text{numérateur}(X_{-1})) = \deg(\text{dénominateur}(X_{-1})) + 1$$

et $d_{-1} = \deg(\text{dénominateur}(L)) + 1 = m$.

3) Montrons que $d_{n-1} + d_{n+1} = 2d_n + 2, \forall n \in \mathbb{Z}$.
1° Considérons d'abord le cas où Z_{n-1}, Z_n ou Z_{n+1} est le point $\mathcal{O}$. Si $Z_{n-1} = \mathcal{O}$, alors $d_{n-1} = 0$ et, par (V.7) et (V.9),

$$Z_n = (x, 1) \text{ et } Z_{n+1} = (x, 1) + (x, 1) = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}, Y_{n+1}\right),$$

et donc $d_n = 1$ et $d_{n+1} = 4$ et la formule est vérifiée. Si $Z_n = \mathcal{O}$, alors $d_n = 0$ et

$$Z_{n+1} = (x, 1) \quad \text{et} \quad Z_{n-1} = -(x, 1) = (-x, 1),$$

et donc $d_{n+1} = d_{n-1} = 1$ et la formule est vérifiée. Si $Z_{n+1} = \mathcal{O}$, alors $d_{n+1} = \mathcal{O}$ et

$$Z_n = -(x,1) = (-x,1) \quad \text{et}$$

$$\begin{aligned} Z_{n-1} &= (-x,1) - (x,1) = 2(-x,1) \\ &= \left(\frac{17x^4 + 14ax^2 + 8bx + a^2}{4(x^3 + ax + b)}, Y_{n-1} \right), \end{aligned}$$

et donc $d_n = 1$ et $d_{n-1} = 4$ et la formule est vérifiée.
2^o Supposons maintenant que Z_{n-1}, Z_n et Z_{n+1} sont tous trois différents de $\mathcal{O}$. Notons

$$X_{n-1} = \frac{A}{B}, \quad X_n = \frac{P}{Q}, \quad X_{n+1} = \frac{C}{D}$$

de sorte que les numérateurs et les dénominateurs n'aient pas de facteur commun, i.e.

$$\text{pgcd}(A,B) = \text{pgcd}(P,Q) = \text{pgcd}(C,D) = 1.$$

Par les formules (V.6) et (V.7), nous avons alors

$$X_{n-1} = \frac{Q^3(1+Y_n)^2(x^3+ax+b) - (Qx-P)^2(P+Qx)}{(Qx-P)^2 Q}, \quad \text{(V.11)}$$

$$X_{n+1} = \frac{Q^3(1-Y_n)^2(x^3+ax+b) - (Qx-P)^2(P+Qx)}{(Qx-P)^2 Q}. \quad \text{(V.12)}$$

En multipliant et en additionnant les deux égalités précédentes, nous obtenons après calculs

$$X_{n-1}X_{n+1} = \frac{(Px-aQ)^2 - 4bQ(Qx+P)}{(Qx-P)^2} = \frac{AC}{BD}, \quad \text{(V.13)}$$

$$\begin{aligned} (X_{n-1} + X_{n+1}) &= \frac{2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]}{(Qx-P)^2} \\ &= \frac{AD+BC}{BD}. \end{aligned} \quad \text{(V.14)}$$

Soit $S = \text{pgcd}(AC, BD)$, alors par (V.13) et (V.14),

$$AC = S[(Px-aQ)^2 - 4bQ(Qx+P)], \quad \text{(V.15)}$$

$$BD = S(Qx-P)^2, \quad \text{(V.16)}$$

$$AD + BC = 2S[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]. \quad \text{(V.17)}$$

Si F est un facteur premier de S, alors, par les relations précédentes,

$$F \mid AC, \quad F \mid BD \quad \text{et} \quad F \mid (AD + BC). \tag{V.18}$$

Supposons que $F \mid B$ (le cas F divise D est symétrique), alors $F \nmid A$ car $\text{pgcd}(A, B) = 1$. De plus, comme $F \mid AC$, il vient que $F \mid C$ et donc $F \mid BC$. Enfin, comme $F \mid (AD + BC)$, il s'ensuit que $F \mid AD$ et $F \mid D$ car $F \nmid A$. Nous avons donc montré que $F \mid C$ et $F \mid D$, par conséquent $F = 1$ car $\text{pgcd}(C, D) = 1$. Par les équations (V.15),(V.16) et (V.17), cela implique que

$$AC = (Px - aQ)^2 - 4bQ(Qx + P), \tag{V.19}$$
$$BD = (Qx - P)^2, \tag{V.20}$$
$$AD + BC = 2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]. \tag{V.21}$$

Nous devons démontrer que $d_{n-1} + d_{n+1} = 2d_n + 2$ ou de façon équivalente que

$$\max(\deg(A), \deg(B)) + \max(\deg(C), \deg(D)) = 2\max(\deg(P), \deg(Q)) + 2.$$

(α) Si $d_{n-1} = \deg(A)$ et si $d_{n+1} = \deg(C)$, alors, par (V.19),

$$d_{n-1} + d_{n+1} = \deg(AC) = \deg[(Px - aQ)^2 - 4bQ(Qx + P)].$$

Par l'absurde, supposons que $\deg(P) < \deg(Q)$. Alors, par (V.20),

$$\deg(BD) = 2\deg(Q) + 2.$$

De plus,

$$\begin{aligned}\deg(AC) &\leq \max(2\deg(P) + 2, 2\deg(Q), 2\deg(Q) + 1, \deg(PQ)) \\ &= 2\deg(Q) + 1 < \deg(BD),\end{aligned}$$

ce qui est impossible. Donc, $\deg(P) \geq \deg(Q)$ et

$$\deg(AC) = \deg(Px^2) = d_n + 2,$$

ce qui démontre le point 3).

(β) Si $d_{n-1} = \deg(B)$ et si $d_{n+1} = \deg(D)$, alors, par (V.20),

$$d_{n-1} + d_{n+1} = \deg(BD) = \deg[(Qx - P)^2].$$

Par l'absurde, supposons que $\deg(Q) < \deg(P)$. Alors, par (V.19),

$$\deg(AC) = \deg(P^2x^2) > \deg(P^2) \geq \deg(BD),$$

ce qui est impossible. Donc, $\deg(Q) \geq \deg(P)$ et

$$\deg(BD) = \deg(Q^2x^2) = d_n + 2,$$

ce qui démontre le point 3).

(γ) Si $d_{n-1} = \deg(A)$ et si $d_{n+1} = \deg(D)$ avec $\deg(A) > \deg(B)$ — sinon, c'est le cas (β) — et $\deg(D) > \deg(C)$ — sinon, c'est le cas (α) —, alors, par (V.21),

$$\begin{aligned}\deg(AD) &= \deg(AD + BC) \quad \text{car } \deg(AD) > \deg(BC)\\ &= \deg\{2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]\}\\ &= \deg(PQx^2).\end{aligned}$$

Si $\deg(P) \geq \deg(Q)$, alors

$$\deg(AD) \leq \deg(P^2x^2) = \deg(AC),$$

ce qui est impossible.
Sinon, si $\deg(P) < \deg(Q)$, alors

$$\deg(AD) < \deg(Q^2x^2) = \deg(BD),$$

ce qui est impossible. Le cas (γ) ne se rencontre donc jamais.

(δ) Si $d_{n-1} = \deg(B)$ et si $d_{n+1} = \deg(C)$ avec $\deg(B) > \deg(A)$ — sinon, c'est le cas (α) — et $\deg(C) > \deg(D)$ — sinon, c'est le cas (β) —, alors, par (V.21),

$$\begin{aligned}\deg(BC) &= \deg(AD + BC) \quad \text{car } \deg(BC) > \deg(AD)\\ &= \deg\{2[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]\}\\ &= \deg(PQx^2).\end{aligned}$$

Si $\deg(P) \geq \deg(Q)$, alors

$$\deg(BC) \leq \deg(P^2x^2) = \deg(AC),$$

ce qui est impossible.
Sinon, si $\deg(P) < \deg(Q)$, alors

$$\deg(BC) < \deg(Q^2x^2) = \deg(BD),$$

ce qui est impossible. Le cas (δ) ne se rencontre donc jamais.

4) Par induction, prouvons que $d_n = n^2 - (d_{-1} - d_0 - 1)n + d_0$.
Pour $n = -1$ et $n = 0$, la relation est trivialement vérifiée. Supposons que $d_{n-2} = (n-2)^2 - (d_{-1} - d_0 - 1)(n-2) + d_0$ et que $d_{n-1} = (n-1)^2 - (d_{-1} - d_0 - 1)(n-1) + d_0$, alors par 3),

$$\begin{aligned} d_n &= 2d_{n-1} - d_{n-2} + 2 \\ &= 2[(n-1)^2 - (d_{-1} - d_0 - 1)(n-1) + d_0] - \\ &\qquad [(n-2)^2 - (d_{-1} - d_0 - 1)(n-2) + d_0] + 2 \\ &= n^2 - (d_{-1} - d_0 - 1)n + d_0. \end{aligned}$$

En remplaçant d_{-1} et d_0 par leurs valeurs calculées en 2), nous obtenons

$$d_n = n^2 + a_p n + p, \tag{V.22}$$

où $a_p = p + 1 - m$.

Considérons la fonction $\rho : \mathbb{R} \to \mathbb{R}, r \mapsto r^2 + a_p r + p$. Si cette fonction a deux racines distinctes r_1 et r_2 avec $r_1 < r_2$, alors $\forall r \in]r_1, r_2[: f(r) < 0$ car $f''(r) > 0$. Or comme $r_2 - r_1 = \Delta = a_p^2 - 4p > 0$ et que a_p est entier, nous avons que $r_2 - r_1 \geq 1$. Il existe donc un entier n tel que $d_n \in]r_1, r_2[$ car deux d_n consécutifs ne peuvent pas s'annuller simultanément. Cela implique que $d_n < 0$, ce qui est impossible car d_n est le degré d'un polynôme. Par conséquent, $\Delta = a_p^2 - 4p \leq 0$ et donc $|a_p| = |p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}$. □

V.1.3 Test de primalité

Le test de primalité utilisant les courbes elliptiques est une variante du test de Pocklington dans $(\mathbb{Z}/N\mathbb{Z})^*$.†

Théorème 72. *Soit N un entier positif. Notons p_i un des facteurs premiers de $N - 1 = \prod_{j=1}^{n} p_j^{e_j}$ et supposons qu'il existe un entier a_{p_i} tel que*

$$a_{p_i}^{N-1} \equiv 1 \pmod{N} \quad \textit{et} \quad \operatorname{pgcd}(a_{p_i}^{(N-1)/p_i} - 1, N) = 1. \tag{V.23}$$

Alors, si d est un facteur de N, $d \equiv 1 \pmod{p_i^{e_i}}$.

Preuve. Comme tout facteur d de N est le produit de nombres premiers, il suffit de démontrer le théorème pour tout facteur premier q de N. Comme $a_{p_i}^{N-1} \equiv 1 \pmod{N}$, il s'ensuit que $uN + a_{p_i}^{N-2} a_{p_i} = 1$. Par le corollaire 4, cela signifie que $\operatorname{pgcd}(a_{p_i}, N) = 1$ et $\operatorname{pgcd}(a_{p_i}, q) = 1$. Nous avons donc

†Nous utilisons la notation $(\mathbb{Z}/N\mathbb{Z})$ et non $\mathbb{F}_N$, car *a priori* nous ne savons pas que $(\mathbb{Z}/N\mathbb{Z})$ est un corps.

$a_{p_i}^{q-1} \equiv 1 \pmod{q}$ par la proposition 64. Notons o_i, l'ordre de p_i modulo q, alors la relation précédente implique que $o_i \mid q-1$. D'autre part, comme $a^{N-1} \equiv 1 \pmod{N}$ et $\operatorname{pgcd}(a_{p_i}^{(N-1)/p_i} - 1, N) = 1$, nous avons

$$\left.\begin{array}{l} a_{p_i}^{N-1} \equiv 1 \pmod{q} \\ a_{p_i}^{(N-1)/p_i} \not\equiv 1 \pmod{q} \end{array}\right\} \Rightarrow o_i \mid p_i^{e_i} \prod_{\substack{j=1 \\ j\neq i}}^{n} p_j^{e_j} \text{ et } o_i \nmid p_i^{e_i-1} \prod_{\substack{j=1 \\ j\neq i}}^{n} p_j^{e_j}$$

$$\Rightarrow o_i\alpha = p_i^{e_i} M \text{ et } o_i\beta \neq p_i^{e_i-1} M \text{ où } M = \prod_{\substack{j=1 \\ j\neq i}}^{n} p_j^{e_j}$$

$$\Rightarrow \alpha \neq p_i\beta$$

$$\Rightarrow p_i^{e_i} \mid o_i.$$

Finalement, nous avons $p_i^{e_i} \mid o_i \mid q-1$, et donc $q \equiv 1 \pmod{p_i^{e_i}}$. □

Corollaire 73 (Critère de Pocklington). *Si q est un facteur premier de $N-1$ strictement supérieur à $\sqrt{N}-1$ et s'il existe un entier a tel que*

$$a^{N-1} \equiv 1 \pmod{N} \quad \textit{et} \quad \operatorname{pgcd}(a^{(N-1)/q} - 1, N) = 1,$$

alors N est premier.

Preuve. Voir corollaire suivant où nous prenons $F = q$. □

Le critère de Pocklington a été affiné par Lehmer de la manière suivante :

Corollaire 74 (Critère de Pocklington-Lehmer). *Si nous pouvons écrire $N-1 = FU$ avec $\operatorname{pgcd}(F,U) = 1$ et $F > \sqrt{N}-1$ et si pour tout facteur premier p_i de F, il existe un a_{p_i} qui satisfait à (V.23), alors N est premier.*

Preuve. Par la proposition précédente, tout facteur de N congrue à 1 modulo F. Les facteurs de N sont donc de la forme $\alpha F + 1$. Or, comme $F > \sqrt{N}-1$, N n'a pas de facteur premier inférieur à sa racine carrée et, par conséquent, N est premier. □

Voyons à présent comment le critère de Pocklington peut être adapté aux courbes elliptiques. Remarquons que nous devons pas travailler avec l'équation générale de Weierstrass. En effet, un simple calcul de pgcd peut nous assurer que N est relativement premier avec 6. Nous allons donc restreindre notre étude à la courbe elliptique E donnée par l'équation de Weierstrass $y^2 = x^3 + ax + b$ plus le point à l'infini $\mathcal{O}$ que nous prendrons comme élément neutre.

Supposons que N soit premier. Afin d'établir l'analogue du critère de Pocklington, comparons les groupes $\mathbb{F}_N^*$ et $(E, \mathcal{O})$:

	$\mathbb{F}_N^*$	$(E, \mathcal{O})$
Éléments	$\{1, 2, \ldots, N-1\}$	$\{(x,y) \in \mathbb{F}_N \mid y^2 = x^3 + ax + b\} \cup \mathcal{O}$
Loi de comp.	$\cdot$ (groupe multiplicatif)	$+$ (groupe additif)
Élément neutre	1	$\mathcal{O} = (0,1,0)$
Cardinalité	$N-1$	m avec $\lvert m - (N+1)\rvert \leq 2\sqrt{N}$

Soit P un point de la courbe elliptique. La condition $a^{N-1} \equiv 1 \pmod N$ devient $mP = \mathcal{O}$; la condition $\text{pgcd}(a^{(N-1)/q} - 1, N) = 1$ peut s'écrire $a^{(N-1)/q} \not\equiv 1 \pmod N$ et devient $\frac{m}{q}P \neq \mathcal{O}$. L'hypothèse q facteur premier de $N-1$ et $q > \sqrt{N} - 1$ demande un peu plus de réflexion. Cette hypothèse est nécessaire pour assurer la primalité de N. Si N avait un facteur premier $p \leq \sqrt{N}$, alors q serait strictement supérieur à $p-1$. De la même manière dans $(E, \mathcal{O})$, un facteur premier q de m doit être supérieur à quelque chose, et ce quelque chose doit être nécessaire pour assurer la primalité de N. Supposons que N ne soit pas premier, alors N possède un facteur premier $p \leq \sqrt{N}$. L'équivalent de la condition $q > p - 1$ deviendrait $q > m'$ où m' est la cardinalité de la courbe E modulo p. Cette dernière condition est satisfaite si $q > (N^{1/4} + 1)^2$ car, par le théorème 71, $m' \leq p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \leq (N^{1/4} + 1)^2 < q$. Rassemblons toutes ces idées dans la proposition suivante :

Proposition 75 (Critère de Goldwasser-Kilian). *Soit N un entier relativement premier avec 6. S'il existe un entier m et un point P de la courbe elliptique*

$$E : y^2 = x^3 + ax + b \pmod N \cup \mathcal{O}$$

tels que

1. *il existe un facteur premier q de m strictement supérieur à $(N^{1/4}+1)^2$,*
2. *$mP = \mathcal{O} = (0,1,0)$,*
3. *$\frac{m}{q}P = (x,y,z)$ avec $z \in (\mathbb{Z}/N\mathbb{Z})^*$,*

alors N est premier.

Preuve. Par l'absurde, supposons que N a un facteur premier p. Notons E' la courbe E modulo p, m' la cardinalité de E' et P' le point de E' correspondant au point P de E. Par hypothèse, $mP = \mathcal{O}$ et $\frac{m}{q}P \neq \mathcal{O}$ sur E et donc,

$$mP' = \mathcal{O} \quad \text{car } p \mid N \tag{V.24}$$

$$\frac{m}{q}P' \neq \mathcal{O} \quad \text{car } z \in (\mathbb{Z}/N\mathbb{Z})^* \tag{V.25}$$

sur E'. Les relations (V.24) et (V.24) impliquent que q divise l'ordre de P' comme point de E' et, par le théorème 7, q divise m'. Il s'ensuit que

$$\begin{aligned} q \leq m' &\leq p + 1 + 2\sqrt{p} = (\sqrt{p}+1)^2 \quad \text{par le théorème 71} \\ &\leq (N^{1/4}+1)^2 \quad \text{car } p \leq \sqrt{N}, \end{aligned}$$

ce qui contredit l'hypothèse. □

Remarque. Nous faisons tous les calculs comme si N était premier. Si l'algorithme de Schoof[†] n'aboutit pas, alors cela signifie que N est composé. De même, dans le calcul de mP et de $\frac{m}{q}P$, il est possible que le dénominateur de λ ne soit pas inversible. Cela signifie que $(\mathbb{Z}/N\mathbb{Z})$ n'est pas un corps, i.e. $(\mathbb{Z}/N\mathbb{Z}) \neq \mathbb{F}_N$, et donc que N est composé. Nous avons alors prouvé que N n'était pas premier.

Exemple 19. Supposons que nous voulions prouver la primalité de 1283 qui a passé avec succès le test de Miller-Rabin. Comme 1283 est relativement premier avec 6, considérons la courbe $y^2 = x^3 + ax + b \pmod{1283}$. Choisissons, par exemple, $x = 121$, $y = 30$ et $a = -1$. Nous calculons alors $b = 30^2 - 121^3 + 21 \bmod 1283 = 0$. Le point $P = (121, 30)$ appartient donc à la courbe

$$E : y^2 = x^3 - x \pmod{1283} \cup \mathcal{O}.$$

Remarquons que cette courbe est non singulière car $\Delta = 64 \neq 0$. Nous devons maintenant calculer le nombre de points de cette courbe. Il n'est pas nécessaire d'utiliser l'algorithme de Schoof, car nous pouvons voir que

$$\chi((-x)^3 - (-x)) = \chi(-1)\chi(x^3 - x) = -\chi(x^3 - x)^{\ddagger}$$

car $1283 \equiv 3 \bmod 4$ et donc

$$\sum_{x \in \mathbb{F}_{1283}} \chi(x^3 - x) = \chi(0) = 0.$$

La cardinalité m de la courbe vaut donc $1283 + 1 = 1284$. Comme $m = 1284 = 12 \cdot 107$, vérifions les hypothèses de la proposition avec $q = 107$:

1. 107 est premier et $107 > ((1283)^{1/4} + 1)^2 \simeq 49$;
2. $1284P = 2(2(P + 2(2(2(2(2(P + 2(2P))))))))) = \cdots = \mathcal{O}$;

[†] Cet algorithme permet de calculer la cardinalité d'une courbe elliptique.

[‡] χ est le caractère quadratique de $(\mathbb{Z}/N\mathbb{Z})^*$, i.e. $\chi(x) = 1$ si x est un carré modulo N et $\chi(x) = -1$ sinon. Nous étendons cette notion à $(\mathbb{Z}/N\mathbb{Z})$ en prenant $\chi(0) = 0$. Remarquons que si N est premier, alors χ est le symbole de Legendre.

3. $\frac{1284}{107}P = 12P = 2(2(P+2P)) = 2(2((121,30)+(1066,377)))$
$= 2(2(1083,1155)) = 2(704,284) = (903,1038) \neq \mathcal{O}$.

Comme toutes les hypothèses sont vérifiées, nous avons prouvé que 1283 est un nombre premier.

Dans cet exemple, nous avons eu la chance que $\frac{m}{q}P \neq \mathcal{O}$. Si ce n'était pas le cas, nous aurions dû considérer un autre point P ou une autre courbe elliptique.

Le gros avantage de la méthode de Goldasser-Kilian par rapport à celle de Pocklington est qu'il est toujours possible, par le théorème 71, de trouver une courbe elliptique dont la cardinalité m vérifie le critère.

V.1.4 Factorisation

La factorisation sur une courbe elliptique est inspirée d'une méthode de factorisation dans $\mathbb{F}_p^*$: l'algorithme $p-1$ de Pollard. Rappelons brièvement cet algorithme.

Définition 76. Un entier N est *B-lisse* si tous les facteurs premiers de N sont inférieurs ou égaux à B. L'entier N est *B-superlisse* si toutes les puissances premières divisant N sont inférieures ou égales à B.

Supposons que le nombre composé N ait un facteur premier p tel que $p-1$ soit B-superlisse, alors, par la proposition 64,

$$a^{\text{ppcm}(1,2,\ldots,B)} \equiv 1 \pmod{p} \quad \forall a \in \mathbb{N} \text{ tel que } \text{pgcd}(a,N) = 1^{\dagger}$$

car $p-1$ divise le plus petit commun multiple des nombres 1 à B. Par conséquent, nous avons

$$l = \text{pgcd}(a^{\text{ppcm}(1,2,\ldots,B)} - 1, N) > 1.$$

Si $l \neq N$, alors nous avons trouvé un facteur non trivial de N, sinon nous calculons l pour une autre valeur de a. Si $l = 1$, alors nous augmentons la valeur de B.

Exemple 20. Supposons que nous voulions factoriser le nombre composé $N = 540143$. Prenons, par exemple, $B = 8$ et $a = 2$ (qui est relativement premier avec N). Le ppcm de $(1,2,\ldots,8)$ est égal à $2^3 \cdot 3 \cdot 5 \cdot 7 = 840$. Calculons

$$\text{pgcd}((2^{840} - 1) \bmod 540143, 540143) = \text{pgcd}(53046, 540143) = 421.$$

Nous avons donc $540143 = 421 \cdot 1283$.

[†] ppcm dénote le plus petit commun multiple.

Le désavantage de cette méthode est qu'il faut que N ait un facteur p tel que $p-1$ soit B-superlisse. Cet inconvénient ne se retrouve pas dans la méthode proposée par Lenstra, basée sur les courbes elliptiques.

Supposons que le nombre composé N ait un facteur premier impair $p > 3$. Nous allons travailler avec la courbe elliptique E :

$$E : y^2 = x^3 + ax + b \cup \mathcal{O} = (0, 1, 0),$$

telle que $E(\mathbb{F}_p)$ soit non singulière. Cette condition est vérifiée en calculant le pgcd du discrimant $\Delta = -16(4a^3 + 27b^2)$ et de N. Si $\text{pgcd}(\Delta, N) > 1$, alors soit $N \mid \Delta$ et nous prenons une autre courbe elliptique, soit Δ et N ont un facteur commun et nous avons trouvé un facteur non trivial de N. Sans perdre de généralités, nous pouvons donc supposer que $\text{pgcd}(\Delta, N) = 1$ et par conséquent que $\Delta \bmod p \neq 0$. Dans la méthode de $p-1$ de Pollard, nous avons supposé que la cardinalité du groupe $\mathbb{F}_p^*$ soit B-superlisse ; de même pour la méthode de Lenstra, nous supposons que la cardinalité m du groupe $E(\mathbb{F}_p)$ soit B-superlisse. Considérons un point $P \neq \mathcal{O} \in E(\mathbb{Z}/N\mathbb{Z})$ et définissons

$$k = \text{ppcm}(1, 2, \ldots, B).$$

Par le théorème 7, nous savons que $kP = \mathcal{O}$ dans $E(\mathbb{F}_p)$ car $m \mid k$ et $P \in E(\mathbb{F}_p)$ (puisque $p \mid N$). Le calcul de kP se fait par la méthode de l'*addition-doublement* telle qu'utilisée dans l'exemple de la page 64. Il suffit d'écrire k en base 2, i.e. $k = (k_{n-1}k_{n-2}\ldots k_0)_2$ avec $k_{n-1} = 1$; le calcul de kP se fait alors comme suit :

$Q = P$
pour $i = n-2$ jusque 0
    $Q \leftarrow 2Q$
    si $k_i = 1$ alors $Q \leftarrow Q + P$
$kP = Q$

Comme le facteur p est inconnu, le calcul de kP se fait dans $E(\mathbb{Z}/N\mathbb{Z})$ et non dans $E(\mathbb{F}_p)$. Il se peut donc, dans le calcul de kP, que λ ne soit pas inversible dans $(\mathbb{Z}/N\mathbb{Z})$. Alors, soit le dénominateur de λ est égal à N et nous prenons alors un autre point P ou une autre courbe elliptique E, soit nous trouvons un facteur non trivial de N en calculant le pgcd du dénominateur de λ et de N. Si le calcul de kP aboutit, alors nous choisissons un autre point P ou une autre courbe elliptique E.

Le seul point délicat de cette méthode est le choix de la courbe elliptique E et de la borne de lissité B. Nous allons montrer sur un exemple comment choisir judicieusement ces paramètres.

Exemple 21. Factorisons à nouveau le nombre $N = 540143$ par la méthode de Lenstra. Soit la famille de courbes paramétrées par a

$$E_a : y^2 = x^3 + ax + 1 \cup \mathcal{O}.$$

Le point $P = (0, 1) \neq \mathcal{O}$ appartient toujours à E_a pour toute valeur de a. Le discriminant Δ vaut $-16(4a^3 + 27)$. Prenons $a = 1$, alors $\text{pgcd}(\Delta, N) = 1$ et la courbe E_1 est bien un courbe elliptique sur $\mathbb{F}_p$ où p est un facteur premier de N. Nous savons que tout facteur premier p de N est inférieur à $\sqrt{N} \simeq 735$. De plus par le théorème 71, le nombre de points de $E(\mathbb{F}_p)$ est majoré par $p + 1 + 2\sqrt{p} < 792$. Nous allons donc prendre $B = 792$ et, par exemple, $k = 2^9 \cdot 3^6 = 373248$ qui est 792-superlisse. Nous calculons ensuite kP par la méthode de l'addition-doublement. Si le calcul aboutit, alors nous augmentons a d'une unité (ou nous augmentons la valeur de B, par exemple, $B = 2^9 \cdot 3^6 \cdot 5^4$) et nous recommençons la procédure, sinon nous avons trouvé un facteur non trivial de N.

L'avantage de cette méthode est que nous allons finir par trouver une courbe elliptique E_a dont la cardinalité est B-superlisse, alors que la méthode de Pollard imposait que $p - 1$ soit B-superlisse.

Il a été montré que la complexité de cet algorithme est en

$$O(e^{(1+\varepsilon)\log N \log\log N}),$$

ce qui le place en tête des algorithmes de factorisation.

V.2 Protocoles cryptographiques

V.2.1 Introduction

Les courbes elliptiques permettent d'implémenter des protocoles cryptographiques semblables à celui proposé par El Gamal.

La sécurité de ces systèmes repose sur la difficulté de calculer un logarithme discret. Mais, contrairement à $\mathbb{F}_q$, il n'existe aucun algorithme subexponentiel pour résoudre le problème du logarithme dans $E(\mathbb{F}_q)$. Cela permet, pour une sécurité équivalente, d'utiliser des clés plus petites.

Par ailleurs, sur un corps choisi, il est possible de construire une multitude de courbes elliptiques. En particulier, si nous travaillons sur une courbe elliptique définie sur $\mathbb{F}_{2^m}$, les calculs se font très rapidement. Les avantages des courbes elliptiques sont donc multiples.

V.2.2 Schéma de Diffie-Helman

Supposons qu'Alice et Bob veuillent échanger une clé pour pouvoir l'utiliser dans un protocole cryptographique quelconque. Ils se mettent d'accord sur un nombre premier p et sur un élément g de $\mathbb{F}_p^*$ qu'ils rendent publique. Alice choisit alors un nombre $x \in \mathbb{F}_p^*$ et Bob, un nombre $y \in \mathbb{F}_p^*$. Les nombres x et y sont respectivement les clés secrètes d'Alice et de Bob. Ensuite, ils calculent respectivement X et Y, qui constituent les clés publiques d'Alice et de Bob, pour obtenir une clé K commune comme l'illustre le schéma suivant.

Alice		Bob
	p, g	
x		y
$X = g^x \bmod p$	$\xrightarrow{X}$	
	$\xleftarrow{Y}$	$Y = g^y \bmod p$
$K = Y^x \bmod p$		$K' = X^y \bmod p$

Figure 8: Schéma de Diffie-Helman classique.

Alice et Bob ont bien la même clé car

$$K \equiv Y^x \equiv (g^y)^x \equiv (g^x)^y \equiv X^y \equiv K' \pmod{p}.$$

Si Caïn est un espion qui observe ce qui se passe (Caïn connaît p, g, X et Y), il ne peut pas obtenir la clé car il n'est pas capable de calculer des logarithmes discrets en un temps raisonnable.

Sur les courbes elliptiques, le schéma est identique si ce n'est qu'Alice et Bob rendent publique une courbe elliptique E définie sur $\mathbb{F}_q$ et un point $P \in E(\mathbb{F}_q)$.

Alice		Bob
	$\mathbb{F}_q, E$	
	$P \in E$	
x		y
$X = xP$	$\xrightarrow{X}$	
	$\xleftarrow{Y}$	$Y = yP$
$K = xY$		$K' = yX$

Figure 9: Schéma de Diffie-Helman elliptique.

Ici aussi, nous pouvons vérifier que la clé est identique car

$$K = xY = x(yP) = y(xP) = yX = K'$$

et un espion ne peut pas calculer la clé K sans résoudre le problème du logarithme.

V.2.3 Codage d'El Gamal

Supposons maintenant qu'Alice veuille envoyer un message à Bob sous forme codée de sorte que Bob soit le seul à pouvoir déchiffrer le message. Avec les notations du paragraphe précédent, notons $m \in \mathbb{F}_p^*$ le message à coder. Alice choisit secrètement un nombre k et calcule $a = g^k \bmod p$. Ensuite, avec la clé publique Y de Bob, Alice calcule $G = Y^k \bmod p$ et $b = Gm \bmod p$. Le message chiffré c est la paire (a, b) qu'elle envoie à Bob. Pour déchiffrer le message, Bob calcule $G = a^y \bmod p$ à l'aide de sa clé secrète y et ensuite retrouve $m = bG^{-1} \bmod p$.

Alice		Bob
	p, g, Y	
m, k		y
$a = g^k \bmod p$		
$G = Y^k \bmod p$		
$b = Gm \bmod p$		
$c = (a, b)$	$\xrightarrow{c}$	$G' = a^y \bmod p$
		$m' = b(G')^{-1} \bmod p$

Figure 10: Codage d'El Gamal classique.

Montrons que Bob retrouve bien le message original m :

$$\begin{aligned} m' &\equiv b(G')^{-1} \equiv Gm(a^y)^{-1} \equiv Y^k m((g^k)^y)^{-1} \equiv (g^y)^k m((g^k)^y)^{-1} \\ &\equiv m \pmod{p}. \end{aligned}$$

La sécurité de ce système repose sur le problème du logarithme ; en effet, Bob est la seule personne capable de calculer G.

Avec les mêmes notations qu'auparavant, l'analogue sur les courbes elliptiques est illustré par le schéma qui suit.

Le message m' calculé par Bob est bien le message m envoyé par Bob car

$$m' = b - G' = b - ya = m + G - ya = m + kY - ykP = m + kyP - ykP = m.$$

Si le message est plus long que les éléments du groupe sur lequel nous travaillons, nous le divisons en plusieurs parties m de la taille des éléments du groupe. Pour chaque partie m, nous effectuons alors la procédure décrite plus haut.

Alice		Bob
	$\mathbb{F}_q, E$	
	$P \in E, Y$	
m, k		y
$a = kP$		
$G = kY$		
$b = m + G$		
$c = (a, b)$	$\xrightarrow{c}$	$G' = ya$
		$m' = b - G'$

Figure 11: Codage d'El Gamal elliptique.

Le désavantage du codage d'El Gamal est que le message chiffré est deux fois plus long que le message clair. Pour parer à cet inconvénient, d'autres méthodes ont été proposé dont le célèbre RSA[†]. Le RSA est basé sur la notion de trappes. Nous n'allons pas présenter ce type de méthodes car il n'y a pas d'analogue, au sens propre, sur les courbes elliptiques : aucune trappe n'est connue pour calculer de manière relativement rapide un logarithme sur une courbe elliptique. Le lecteur désireux d'en apprendre plus consultera [17].

V.2.4 Représentation d'un message

Dans le codage d'El Gamal, nous n'avons pas expliquer comment représenter le message m sur la courbe elliptique E. Il n'existe aucune méthode déterministe pour représenter un message ; néanmoins, il est possible de fixer la probabilité d'échec. Pour fixer les idées, notons

$$E : y^2 = x^3 + ax + b \cup \mathcal{O},$$

la courbe elliptique sur $\mathbb{F}_q$ et k tel que 2^{-k} est la probabilité qu'on ne puisse pas représenter le message m. Supposons que

$$\text{(i) } m < M \quad \text{et} \quad \text{(ii) } q > Mk.$$

Nous représentons le message m comme un élément de $\mathbb{F}_q$ par

$$\widetilde{x} = mk + j,\ 1 \leq j \leq k.$$

Remarquons que $\widetilde{x} \leq (M-1)k + k = Mk < q$. Nous choisissons alors $\widetilde{y}$ tel que

$$\widetilde{y} = \widetilde{x}^3 + a\widetilde{x} + b$$

[†]RSA pour les initiales de ses inventeurs : Rivest, Shamir et Adleman.

soit un carré en essayant $j = 1, 2, \ldots, k$. Pour retrouver le message m, Bob calcule

$$\left\lfloor \frac{\widetilde{x} - 1}{k} \right\rfloor = m.$$

Comme il y a approximativement une chance sur deux pour que $\widetilde{y}$ soit un carré, la probabilité d'échec est de l'ordre de 2^{-k}.

À retenir.

- (Théorème de Hasse) Si E est une courbe elliptique définie sur $\mathbb{F}_q$, alors
$$q + 1 - 2\sqrt{q} \leq \#E(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}.$$
- Les tests de primalité sur les courbes elliptiques tirent parti du théorème de Hasse et aboutissent là où les tests "classiques" échouent.
- Les courbes elliptiques permettent de factoriser en un temps polynomial. Cependant, elles permettent seulement de trouver des facteurs premiers ayant moins de 70 chiffres décimaux (les méthodes "classiques" sont limitées à 20 chiffres décimaux).
- Tous les protocoles cryptographiques classiques existants peuvent être adaptés avec plus ou moins de succès sur les courbes elliptiques. Le gros avantage de ces dernières est que la taille des clés est plus petite pour une sécurité équivalente et qu'il est possible de travailler sur $\mathbb{F}_{2^m}$.

Conclusion

Nous voilà arrivés au terme du rapport. La présentation et les démonstrations ont été faites dans le but d'être compréhensibles par quiconque ayant un bagage minimum en mathématiques. Des démonstrations plus concises et plus élégantes peuvent être trouvées dans le livre de Silverman [19] qui s'est imposé comme étant la "bible" sur le sujet. Je recommande donc très vivement de le consulter pour découvrir davantage sur les courbes elliptiques. Un autre livre qu'il est utile de consulter est celui de Husemöller [9] qui, bien qu'étant moins complet que le premier, est plus facile à lire.

Remerciements

N'étant pas un spécialiste dans le domaine des courbes elliptiques, je n'aurai pas pu effectuer un tel travail sans le soutien professionnel et moral de plusieurs personnes et institutions.

Je ne saurais trop remercier Jean-Jacques Quisquater, mon promoteur, pour m'avoir fait découvrir la cryptologie et la théorie des nombres. Je le remercie plus particulièrement de m'avoir donné l'opportunité de suivre le cours de théorie algorithmique des nombres à l'École Polytechnique (Palaiseau) [6] et d'assister à Eurocrypt '95.[†]

Merci également à Francis Borceux, mon copromoteur, pour l'excellent travail de fond qu'il a fait. Je me suis en effet très fortement inpiré de ses notes [2] pour l'élaboration de ce rapport. Par ailleurs, je remercie l'unité AGEL pour avoir pu assister au colloque de théorie algébrique des nombres à Besançon.

Enfin, je remercie le département de mathématiques et d'informatique de l'École Normale Supérieure (Paris) pour son accueil lors de mes séjours et en particulier Jean-Marc Couveignes pour avoir su m'expliquer patiemment ce qu'il connaissait sur les courbes elliptiques.

Marc Joye.

[†]Avec la collaboration de Benoît Macq.

Références

[1] Francis Borceux. *Invitation à la géométrie.* Ciaco, Louvain-la-Neuve, 1986.

Ce livre présente tous les aspects de la géométrie de la "préhistoire" à nos jours. Le chapitre XII (La naissance de la géométrie algébrique) est particulièrement intéressant.

[2] Francis Borceux and Jean-Jacques Quisquater. *Number theory and cryptology.* To appear.

La troisième partie de ce livre (Elliptic curves) présente la théorie des courbes elliptiques d'un point de vue géométrique. Il constitue une excellente introduction à ce mémoire, qui s'en est d'ailleurs très fortement inspiré.

[3] David M. Bressoud. *Factorization and primality testing.* Undergraduate Texts in Mathematics. Springer-Verlag, 1989.

Ce livre couvre de façon élémentaire presque tous les algorithmes de pseudo-primalité, de primalité et de fatorisation. On y trouve également un résumé sur les courbes elliptiques sur les corps finis.

[4] Robert D. Carmichael. *Introduction to the theory of groups of finite order.* Dover Publications, Inc., 1956.

Ce livre introduit la théorie des groupes et en démontre les théorèmes fondamentaux.

[5] Henri Cohen. *A course in computational algebraic number theory.* Number 138 in Graduate Texts in Mathematics. Springer-Verlag, 1993.

Ce livre couvre tous les domaines de la théorie algébrique des nombres d'un point de vue algorithmique. Tous les algorithmes vus dans ce mémoire y sont décrits et ont été implémentés dans Pari qui est disponible par ftp anonyme à ftp.inria.fr.

[6] Jean-Marc Couveignes and François Morain. Théorie algorithmique des nombres. Notes de cours.

Ce cours est semblable à [2], si ce n'est que l'accent est davantage mis sur l'aspect algorithmique.

[7] William Fulton. *Algebraic curves.* W. A. Benjamin, Inc., 1969.

La lecture de ce livre est nécessaire comme introduction à [19]. En particulier, le chapitre 8 (Riemann-Roch theorem) permet de démontrer par la théorie des diviseurs qu'à toute cubique non singulière peut être associée une structure de groupe.

[8] Roger Godement. *Cours d'algèbre.* Hermann, 3rd edition, 1966.

Ce livre constitue un excellent résumé d'algèbre, il est à la fois précis et facile à lire.

[9] Dale Husemöller. *Elliptic curves.* Number 111 in Graduate Texts in Mathematics. Springer-Verlag, 1987.

Ce livre est très bien écrit et couvre quasi tous les domaines ayant trait aux courbes elliptiques. Certains chapitres sont néanmoins difficiles.

[10] W. E. Jenner. *Rudiments of algebraic geometry.* Oxford University Press, 1963.

Ce petit livre introduit de manière très élémentaire les notions de géométrie algébrique.

[11] Anthony W. Knapp. *Elliptic curves.* Number 40 in Mathematical Notes. Princeton University Press, 1992.

La plupart des chapitres utilisent des arguments de nature géométrique. Les démonstrations sont par conséquent assez faciles mais pas toujours très éclairantes.

[12] Neal Koblitz. *Introduction to elliptic curves and modular forms.* Number 97 in Graduate Texts in Mathematics. Springer-Verlag, 1984.

Ce livre fournit plusieurs outils nécessaires pour traiter les courbes elliptiques et les formes modulaires.

[13] Neal Koblitz. *A course in number theory and cryptography.* Number 114 in Graduate Texts in Mathematics. Springer-Verlag, 2nd edition, 1994.

Ce livre fait un tour d'horizon de la théorie des nombres et de ses applications liées à la cryptographie.

[14] Serge Lang. *Elliptic functions.* Addison-Wesley Publishing Company, Inc., 1973.

Ce livre constitue une excellente introduction aux fonctions elliptiques.

[15] Reynald Lercier and François Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In Louis C. Guillou and Jean-Jacques Quisquater, editors, *Advances in Cryptology – EUROCRYPT '95*, number 921 in Lecture Notes in Computer Science, pages 79 – 94. Springer-Verlag, 1995.

Cet article présente l'état de l'art pour calculer le nombre de points sur une courbe elliptique définie sur un corps fini.

[16] Robert J. Mc Eliece. *Finite fields for computer scientists and engineers.* Number 23 in Kluwer international series in engineering and computer science. Kluwer Academic Publishers, 1987.

Ce livre est semblable à [4] si ce n'est qu'il est illustré par de nombreux exemples tournés vers l'ingénieur.

[17] Alfred Menezes, Minghua Qu, and Scott Vanstone. IEEE P1363, chapter 6. Available via anonymous ftp at ftp.rsa.com. April 1995.

Ce papier constitue une proposition de standardisation des protocoles cryptographiques appliqués aux courbes elliptiques. Une annexe mathématique introduit de façon succinte les notions élémentaires sur les courbes elliptiques.

[18] Hans Riesel. *Prime numbers ans computer methods for factorization*, volume 57 of *Progress in mathematics.* Birkhäuser, 1985.

Ce livre est comparable à [3]. La présentation est cependant davantage tournée vers l'implémentation.

[19] Joseph H. Silverman. *The arithmetic of elliptic curves.* Number 106 in Graduate Texts in Mathematics. Springer-Verlag, 1986.

Ce livre est *la* référence dans le domaine. Néanmoins, de nombreuses lectures complémentaires s'imposent car le niveau est assez élevé.

[20] Joseph H. Silverman and John Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer-Verlag, 1992.

Sans doute le livre le plus facile à lire sur les courbes elliptiques. Il doit être lu avant de s'attaquer à un ouvrage plus sérieux comme [9] ou [19].

[21] Robert J. Walker. *Algebraic curves.* Springer-Verlag, 1950.

Ce livre présente de manière relativement simple la théorie des courbes algébriques.